DEPARTMENT OF THE ARMY
U.S. ARMY SPACE & MISSILE DEFENSE COMMAND
64 Thomas Johnson Drive
FREDERICK, MD 21702

REPLY TO ATTENTION OF:

Chemical and Biological Agents Branch

SUBJECT: Memorandum for Draft Request for Proposal No. W9113M-06-R-0011

You are invited to submit comments in response to the Draft Request for Proposals (DRFP) No. W9113M-06-R-0011. This requirement is for the procurement of installation and testing of the Integrated Commercial Intrusion Detection System-IV (ICIDS-IV), for the equipment, site survey, facility preparation, site installation, engineering support, testing, warranty, training and technical data, site design, commercial equipment manufacture and deployment and maintenance of ICIDS-IV. The ICIDS-IV is a detection system used to monitor designated areas and facilities on and around an installation. When unauthorized attempts to enter these areas and facilities are detected, the ICIDS-IV provides alarms for operators to take required action. The objective of the ICIDS program is to provide a standard configuration for all military installations located in CONUS and OCONUS. ICIDS-IV consists of Commercial Off-the-Shelf (COTS) equipment, to include interior and exterior sensors, Primary Monitor Consoles (PMC), Remote Status Monitors (RSM), Remote Area Data Collectors (RADC), Closed Circuit TV (CCTV), and Entry Control Equipment (ECE). Responses to this DRFP are voluntary, intended for Government use only and not for public release.

1. Federal Acquisition Regulation provision 52.215-3 is applicable and states:

52.215-3 --Request for Information or Solicitation for Planning Purposes (Oct 1997)

(a) The Government does not intend to award a contract on the basis of this draft solicitation or to otherwise pay for the information solicited except as an allowable cost under other contracts as provided in subsection 31.205-18, Bid and proposal costs, of the Federal Acquisition Regulation.

(b) Although “proposal” and “offeror” are used in this Request for Information, your response will be treated as information only. It shall not be used as a proposal.

(c) This solicitation is issued for the purpose of: Procurement of installation and testing of the Integrated Commercial Intrusion Detection System-IV (ICIDS-IV).

(End of Provision)

2. A draft for Solicitation Sections C (Statement of Work), L (Instructions to Offerors) and M (Evaluation Criteria for Award)) are provided for industry review and comment. Also, the following referenced documents are being provided: Acronym List, Performance Specifications (ICIDS-PS-0600, 0601, 0602); Tentative ICIDS-IV Distribution Plan (forecasted installation sites); Attachment A (Requirements for Development and Production of Equipment Publications); and equipment Performance Equivalency Sheets (PES). Prospective offerors are encouraged to:

a. Provide technical and business feedback on DRFP content, format, clarity, and any other aspects that are relevant to this solicitation to provide improvements in methodology to fulfill the ICIDS-IV mission.

b. Suggest contract type, CLIN structure and contract incentives that would provide the impetus for maximum industry interest, as well as be most advantageous to the Government. Explain the basis for the suggested contract type and incentive.

c. Identify and or suggest cost effective commercial warranty programs that would be available to the Government.

d. Suggested schedule of events for prospective Performance Based Payments.

3. Please provide a point of contact (phone number & email address) for discussing comments submitted in response to the DRFP. Prospective offerors should email their response to the address shown below, to be received no later than 4:00 p.m., EST on March 6, 2006.

Greg.florey@det.amedd.army.mil

4. Upon completion of the Governments review of responses to the DRFP, a Final Request for proposal (RFP) is expected to be issued on or about March 31, 2006. With the final RFP, documentation for the "pseudo-site" will be provided. Offeror responses to this requirement identified in Section L, will be one of the primary elements utilized by the Government to evaluate the offeror's technical and cost approach for contract award. The final RFP will be available at the following website:

http://www.smdc.army.mil/contracts/contracts.html

5. Questions related to this DRFP may be addressed to Mr. Greg Florey at (301)619-8427 or by Email: greg.florey@det.amedd.army.mil

STATEMENT OF WORK (SOW) FOR THE

INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEM-IV (ICIDS-IV)

Final DRAFT

16 February 2006

1.0 SCOPE

1.1 General

This Statement of Work (SOW) applies to the Integrated Commercial Intrusion Detection System-IV (ICIDS-IV), which consists of Commercial Off-The-Shelf (COTS) equipment, to include interior and exterior sensors, Primary Monitor Consoles (PMC), Remote Status Monitors (RSM), Remote Area Data Collectors (RADC), Closed Circuit TV (CCTV), and Entry Control Equipment (ECE).

1.2 ICIDS-IV Effort

The Contractor shall provide an installed ICIDS-IV and associated equipment and material that integrates the Contractor Furnished Equipment (CFE) and any existing Government installed equipment. This effort includes:

- Provide test and evaluation laboratory
- Performing IDS Site Survey.
- Site Specific Design efforts.
- Providing all installation materials and labor
- Installing and acceptance testing each ICIDS-IV system.
- One Year Warranty including parts and labor.
- Operator and Systems Administrator Training.
- Developing and providing associated data.
- Providing technical support during Government conducted system performance verification and Government endurance testing
- Site preparation, if required (when approved by the Government).
- Provide Technical Manuals.

1.3 ICIDS-IV Sites

The sites at which the ICIDS-IV shall be delivered and installed may be located inside or outside the contiguous United States (CONUS). The tentative ICIDS-IV Distribution Plan is listed in attachment J. Potential Air Force and Navy sites for the installation of ICIDS-IV are to be determined (TBD).Contractor will need to coordinate theater clearance requirements for OCONUS sites.

1.4 ICIDS-IV Delivery Orders

The contractor shall be prepared to propose and execute individual delivery orders after contract award to include management, survey and design, installation, testing, and modifications.

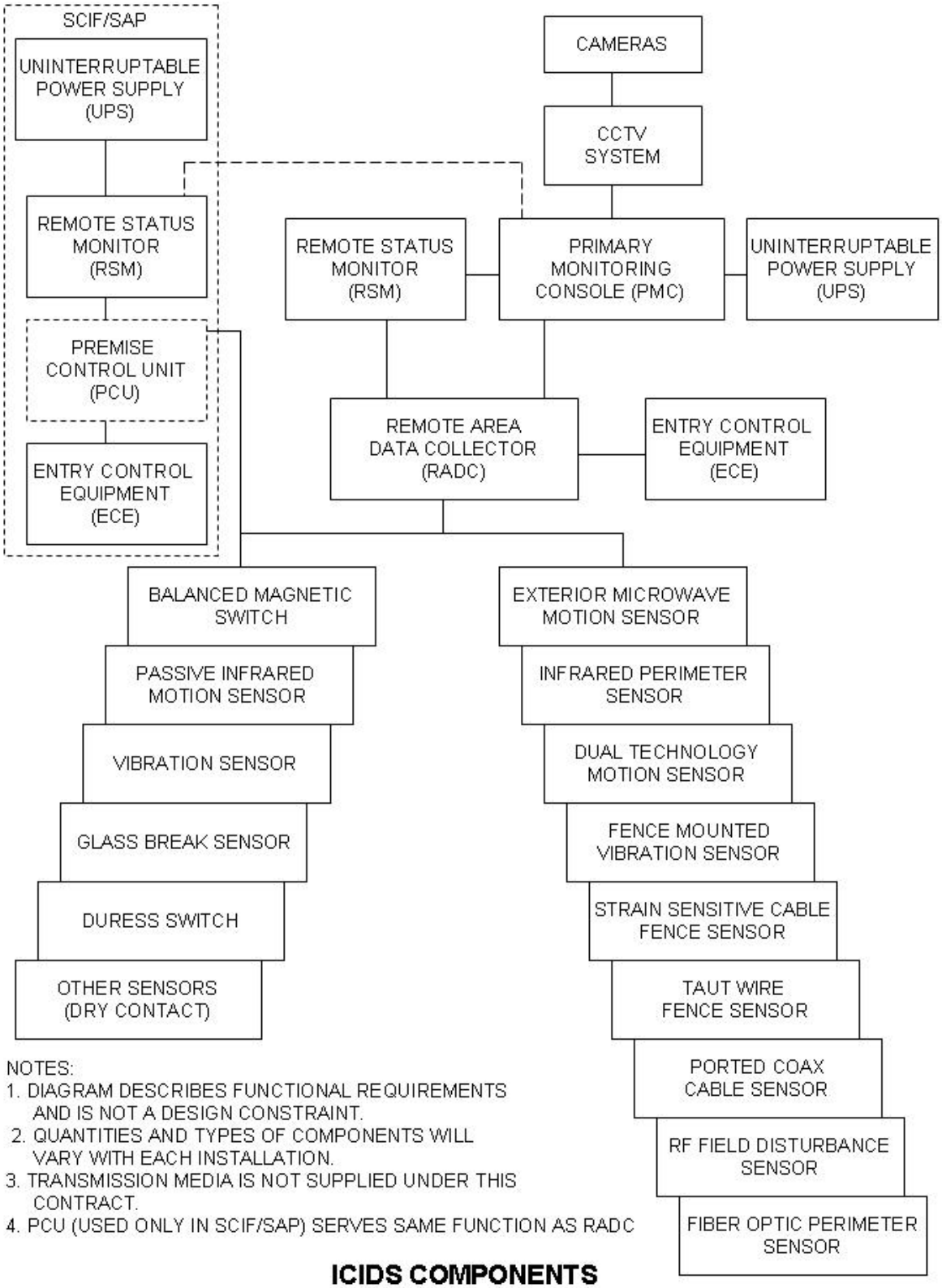

SCIF/SAP
UNINTERRUPTABLE POWER SUPPLY (UPS)
REMOTE STATUS MONITOR (RSM)
PREMISE CONTROL UNIT (PCU)
ENTRY CONTROL EQUIPMENT (ECE)
CAMERAS
CCTV SYSTEM
REMOTE STATUS MONITOR (RSM)
PRIMARY MONITORING CONSOLE (PMC)
UNINTERRUPTABLE POWER SUPPLY (UPS)
REMOTE AREA DATA COLLECTOR (RADC)
ENTRY CONTROL EQUIPMENT (ECE)
BALANCED MAGNETIC SWITCH
PASSIVE INFRARED MOTION SENSOR
VIBRATION SENSOR
GLASS BREAK SENSOR
DURESS SWITCH
OTHER SENSORS (DRY CONTACT)
EXTERIOR MICROWAVE MOTION SENSOR
INFRARED PERIMETER SENSOR
DUAL TECHNOLOGY MOTION SENSOR
FENCE MOUNTED VIBRATION SENSOR
STRAIN SENSITIVE CABLE FENCE SENSOR
TAUT WIRE FENCE SENSOR
PORTED COAX CABLE SENSOR
RF FIELD DISTURBANCE SENSOR
FIBER OPTIC PERIMETER SENSOR
NOTES:
1. DIAGRAM DESCRIBES FUNCTIONAL REQUIREMENTS AND IS NOT A DESIGN CONSTRAINT.
2. QUANTITIES AND TYPES OF COMPONENTS WILL VARY WITH EACH INSTALLATION.
3. TRANSMISSION MEDIA IS NOT SUPPLIED UNDER THIS CONTRACT.
4. PCU (USED ONLY IN SCIF/SAP) SERVES SAME FUNCTION AS RADC
ICIDS COMPONENTS

Figure 1

2.0 APPLICABLE DOCUMENTS

The documents listed in this section form a part of this SOW to the extent specified by specific reference in other paragraphs of this SOW. If a document is referenced without indicating any specific paragraph as being applicable, then the document is applicable in its entirety.

2.1 Government Documents

Department of Defense (DoD) Directive Number 3224.3	17 Feb 89	Physical Security Equipment (PSE) Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support.
Army Regulation (AR) 190-13	30 Sept 93	The Army Physical Security Program
*Operational Requirements Document (ORD)	04 Oct 94	Integrated Commercial Intrusion Detection System (Revised)
**System Performance Specification (Documents listed below)		Integrated Commercial Intrusion Detection System – IV
ICIDS-PS-0600	31 Oct 05	Performance Specification (PS) for Command, Control, and Display Subsystem of the Integrated Commercial Intrusion Detection System
ICIDS-PS-0601	31 Oct 05	Performance Specification for Closed Circuit Television Assessment Equipment of the Integrated Commercial Intrusion Detection System.
ICIDS-PS-0602	31 Oct 05	Performance Specification for Entry Control Equipment of the Integrated

		Commercial Intrusion Detection System.
*DCID 6/9	18 Nov 02	Physical Security Standards for Sensitive Compartmented Information Facilities
*JAFAN 6/9	23 Mar 04	Joint Air Force-Army-Navy Physical Security Standards for Special Access Program Facilities
AR 380-381	21 Apr 05	Special Access Programs (SAPs) and Sensitive Activities
AR 190-59	01 Jul 98	Chemical Agent Security Program
DODI 5200.40	30 Dec 97	DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
AR 190-11	12 Feb 98	Physical Security of Arms, Ammunition and Explosives
DoD Directive (DoDD) 8500.1	**24 Oct 02**	**Information Assurance (IA)**
DoD Directive (DoDD) 8500.2	**6 Feb 03**	**Information Assurance (IA) Implementation**
DoD Instruction (DoDI) 8500.1	**24 Oct 02**	**Information Assurance (IA)**
DoD Instruction (DoDI) 8580.1	**09 Jul 04**	**Information Assurance (IA) In The Defense Acquisition System**
DoD 8510-1M	**31 Jul 00**	DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual

- *= Offerors may contact the Contracting Office if not able to find on the WWW.
- **=Documents attached to the RFP

2.2 Military Specifications and Standards

MIL-STD-40051-2	Department of Defense Standard Practice: Preparation of Digital Technical Information for Page Based Technical Manuals

MIL-STD-38784 (Including Notices 1&2)	Department of Defense Standard Practice for Manuals, Technical: General Style and Format Requirements

NOTE: MIL-STD-40051-2 will govern technical content requirements only; MIL-STD-38784 will govern style and format requirements only.

*MIL-STD-882	System Safety Program Requirements

Asterisked (*) items are to be used for guidance, use is not mandatory.

Unless otherwise indicated, electronic copies of the above documents are available from: http://assist.daps.dla.mil/quicksearch/.

Hard copies can be obtained from:
Standardization Documents Order Desk
700 Robbins Avenue, Building 4D
Philadelphia, PA 1911-5094

2.3 Order of Precedence

In the event of a conflict between the text of this document and the references cited herein, the text of this document (SOW) takes precedence followed by ICIDS Performance Specifications, Site specific design, and associated drawings. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3.0 REQUIREMENTS

3.1 General

Unless otherwise provided, the Contractor shall furnish all personnel, materials and services necessary to accomplish the timely fielding of the ICIDS-IV in accordance with the contract and resulting delivery orders.

3.2 Program Management

3.2.1 Planning and Scheduling. The Contractor shall implement, manage, update, and maintain a schedule that shall be presented for discussion at each Program Status Review (PSR) meeting and contained in the Monthly Status Report IAW Contract Data Requirements List (CDRL) A001. The Contractor shall produce and install ICIDS-IV in accordance with contractor's Government approved plan and schedule. The plan and schedule shall be used throughout the contract as a management tool to assess progress and status relative to achieving program requirements. The Contractor shall also report on work in progress at PSR meetings and in the Monthly Status Report (CDRL) A001. The location for each meeting shall be the Government's facility, Ft. Belvoir, VA.

3.2.2 The Contractor shall host a Start-of-Work meeting, within 30 days of contract award. The Agenda with discussion issues will be sent to the Government for approval within 7 workdays prior to scheduled Start-of-work meeting. This meeting shall be held at contractor's facility. Discussions will take place about the ICIDS-IV program, the first Delivery Order events and timeline, as well as Technical Manual (TM) and training program/materials development.

3.2.3 The contractor shall be responsible for recording the minutes of all meetings held with the Government. The minutes shall be submitted in accordance with CDRL A035.

3.3 Engineering Support

a. Engineering support consists of site surveys, site specific designs, systems installations, and software/hardware engineering support to the installed sites as defined below. Labor categories to be used in performing the engineering support will be proposed by the contractor and subject to review by the Government for reasonableness, will be included in Section B of the contract award. (FP & Contracts will need to finalize this issue G.F.)

b. Contractors shall establish and maintain a fully operational IDS test and evaluation laboratory for the duration of the contract. The laboratory shall be available to the Government for training and demonstration and located not greater than 30 miles from Fort Belvoir, VA.

3.3.1 Site Survey

a. When the Government identifies a requirement IAW Department of Army, Office of Provost Marshal General (OPMG) prioritized fielding plan, the Contracting Officer (KO) will issue the contractor a delivery order. The Contractor shall be provided the following by Product Manager-Force Protection Systems (PM-FPS):

(1) Available Government site drawings,

(2) contact information for the Government Site Point of Contact (SPOC), the security office for passing security clearances of all contractor personnel, SPOC will assist in coordinating,

(3) a list of all currently installed intrusion detection equipment (IDS),

(4) and a list of all locations on the site that require IDS.

b. The Contractor shall submit a proposal with supporting rationale for the work-hours for labor categories and travel/subsistence price proposed, in compliance with Joint Travel Regulations, web site "https://secureapp2.hqda.pentagon.mil/perdiem/trvlregs.html" to accomplish the Site Survey and Site Specific Design (SSD).

3.3.1.1 Performance of Site Survey

For the site survey, the Contractor shall visit the site and use a checklist to perform a detailed site survey to determine equipment type, quantities, and locations needed to provide a complete

ICIDS-IV system to support the site requirements. The survey shall identify necessary site preparations requirements, and defining hardware and/or software interfaces with existing Intrusion Detection Systems (IDS) or other security equipment. The contractor shall identify all existing IDS equipment that is not operating or state-of the-art for replacement during the ICIDS-IV installation. All documented information, such as drawings and lists of existing equipment, shall be verified by comparison with actual existing conditions at each site. Additionally, as a part of the site survey, the Contractor shall verify availability and certify the quality of any Government furnished Data Transmission Media (DTM), low voltage transmission lines and electrical grounding systems. All DTM and Radio Links shall be tested to determine suitability for use in the ICIDS-IV communication system. The site survey report shall document differing site conditions IAW FAR 52.236-3 Site Investigation and Conditions Affecting the Work for submission to the government IAW CDRL A002.

The site survey is the most critical factor for the successful completion of system installation for providing an operationally available and secure IDS. It is necessary that the site survey team be qualified in all aspects of the survey process including management oversight, technical capability, certified electrician and previous IDS site survey experience. Contractor shall provide proof of qualification (diploma, certifications, licenses, skill set, experience installing similar commercial security systems, etc…) for the Program Manager, Site Managers, Engineers, Technicians, Electricians, Quality Control and Configuration Management, or equivalent.

3.3.1.2 Site Survey Report

After the Government issues the first Delivery Order for a Government site location requirement, the Contractor shall submit a Site Survey Report and Engineering Plan IAW CDRLs A002 and A003. This report shall include findings of the site survey, and clearly point out any discrepancies. Site conditions, new facilities, or other changed requirements shall be fully documented in detail. New floor plans, changed equipment layouts, revised block diagrams, preliminary price data for the equipment and installation, and other data shall be included to fully document the recommendations. In addition, the Contractor shall identify any extreme environmental conditions that would exceed the operational limits of equipment to be installed. The report shall also document the results of the DTM tests, identifying links that are suitable and those unsuitable for use in the ICIDS-IV. Should unsuitable DTM be identified, the report shall make recommendations for either using alternative DTM or re-conditioning/replacing the existing DTM.

3.3.1.3 Site Preparation Requirements and Installation Plan

The Contractor shall submit a Site Preparation Requirements and Installation Plan - Design IAW CDRL A004. This document shall specifically denote site preparation requirements to support system installation and required completion dates of site preparation projects. The installation will be responsible for site preparation unless the site preparation required is part of a turnkey as specified by the Government. This Site Preparation Requirements and Installation Plan shall clearly identify a logical schedule of significant events for system installation, including site preparation responsibility, definition of lay down areas, contractor mobilization, facility access, planned utility interruptions, system startup, checkout, projected test schedules, and other tasks required to accomplish the ICIDS-IV installation. Contractor is responsible for daily clean up IAW FAR clause 52.236-12 and contractor shall be in compliance with all safety regulations and codes.

3.3.1.4 Site Specific Design (SSD)

The design shall provide a complete description of the ICIDS-IV system design. The design documentation package shall include required drawings, a design analysis, preliminary pricing estimate, and any other data required to support the design.

a. Drawings. The drawing package shall include IAW CDRL A005:

(1) Title sheet (100 percent complete).

(2) Index of abbreviations and symbols along with definitions (100 percent complete).

(3) Site plan (100 percent complete).

(4) ICIDS-IV block diagram, including data link interface with the installation's DTM (100 percent complete).

(5) ICIDS-IV zones and sensor installation design including definition of existing equipment to be removed (Paragraph 3.3.5) and equipment to be interfaced with ICIDS-IV.

(6) CCTV assessment block diagram, if applicable, after site survey is complete. (100 percent complete).

(7) Entry control system block diagram, if applicable, after site survey is complete. (100 percent complete).

(8) Site Security Center equipment layout and arrangement (100 percent complete).

b. Design analysis. The design analysis shall include a narrative discussion of design philosophy and assumptions, reference sources, and design calculations. It shall also outline the alternative systems, arrangements, and hardware that were considered in arriving at the recommended concept design, and the rationale for selection of alternatives.

c. Preliminary installation hours and materials estimate. As a minimum, this shall include price estimates of the following:

(1) ICIDS-IV components and materials, installation components/hardware, and bulk installation materials.

(2) Hours and labor categories required for necessary removal, disposal of any existing equipment and installation of ICIDS-IV components, materials, and testing.

(3) Travel/subsistence. Rates shall be in accordance with Joint Travel Federal Regulations; state justification for Travel, etc.

(4) Justify rental equipment and rates used during installation.

(5) Required modifications/repair of any existing IDS that is needed to interface with the ICIDS-IV.

d. Design Documentation. Upon Government review and comment on the draft, the contractor shall provide the SSD for Government approval. The contractor shall describe in detail the changes made between the draft and SSD.

3.3.2 Site Installation

Upon Government approval of the SSD, the Contractor shall submit a proposal for the Site Specific Installation. It shall include supporting rationale for the work-hours and travel/subsistence proposed to accomplish the Site Installation effort; including removal of existing IDS equipment as identified in the Government approved Site Survey Report and Engineering Plan. It shall also include a documented schedule, with supporting rationale, of all ICIDS-IV components and materials, and installation rental equipment required for installation IAW the approved SSD. Upon Government approval of the proposal, the Contracting Officer will issue a separate delivery order for the Site Installation. The Contractor shall then proceed with the Site Installation effort. During the changeover of operational mission from existing IDS to the ICIDS-IV the contractor shall not cause any portion of the system to be "down" (i.e., non-operational) for more than 48 hours, with not more than 10 percent of the system being "down" at any one time. The date of initiation of Site Installation work shall be determined upon final acceptance by the Government of the Contractor's submitted SSD and completion of any required site preparation. Installation shall be completed within the time set forth in the delivery order that funds the Site Installation effort. The ICIDS-IV shall be installed IAW the Government approved SSD. Prior to Government acceptance of the installed system, the Contractor shall revise SSD drawings to reflect actual installed design IAW CDRL A006. The as-built drawings shall accurately reflect all field changes.

Each installation will provide the Contractor with suitable storage and office workspace IAW the agreed upon terms and conditions set forth in the Memorandum Of Notification between the Product Manager-Force Protection Systems and the gaining commander. If the Government cannot provide suitable storage and office space as determined during the Site Survey the contractor shall identify and propose an alternate plan to include possible location off site. The Contractor shall remove all debris at the end of each shift, or more frequently if required, to keep the space safe and useable at each site. After installation, the Contractor shall restore the area to a clean condition, dispose of packing material and installation debris, and repair any Contractor caused damage to Government property.

3.3.3 Interruption of Utility Services

All intentional interruptions of utility services shall be scheduled with the Government SPOC. The Contractor shall make every effort to prevent any unintentional interruption of services.

3.3.4 Equipment Delivery and Storage

The Contractor shall be responsible for the preparation and delivery of all required installation materials and equipment, and shall perform loading, unloading, packing, unpacking, inventory, and inspection of said equipment at each site. The Contractor shall also be responsible for proper storage of all materials and equipment security under its cognizance during performance of this contract.

3.3.5 Removal of Installation Debris

The Contractor shall be responsible for the removal and disposal of all debris generated as the result of the installation including removed equipment in accordance with the Delivery Order (D.O.).

3.4 Software Requirement

3.4.1 System Application Software.

The ICIDS-IV Contractor shall provide both system and application (COTS) software. The system software shall support the application software programs. The system software, in general, shall include: system start-up with bootstrap and loader; a disk operating system with program control functions, error detection and recovery, device drivers, file management, CD management, and editor software; utility software for disk compression; diagnostic programs; user access controls; and remote computer control software. The application software shall provide the interface between the alarm acknowledgment, remote secure zone access/secure activation, system test, report generation, and graphic display generation. In addition, the application software shall provide system access control; alarm monitoring program; graphic display software; system test software; a report generator; operator prompt program; closed circuit television interface program, and entry control equipment interface program. If a software license is required, a one-time site license for all ICIDS-IV installations shall be offered.

3.4.2 Software Defect Corrections.

All corrections to software defects (which are defined as any failure or inability to meet the system's requirements) shall be made available and installed at no change in contract price or performance period extension. See Paragraph 3.9.2 for hardware and software upgrades.

3.4.3 System Software.

Upon successful completion of the Performance Verification Test (PVT) and subsequent System Acceptance Test (SAT), (Paragraphs 4.2.2 and 4.2.4, respectively), the Contractor shall provide original and backup (operational, application, support, and diagnostics) software and instructional documentation IAW CDRL A008.

3.5 Documentation Requirements

3.5.1 Product Bulletins

The Contractor shall deliver product bulletins, as an attachment to the Monthly Status Report (CDRL A001), which shall identify existing and potential problems and contractor recommend solutions on each D.O., and provide information on any changes to the ICIDS-IV hardware, software, training materials, or service provided under this contract, including new releases and lessons learned. FAR clause 52.216-2 Economic Price Adjustment-Standard Supplies, shall be followed for supplies.

3.5.2 Technical Manuals

The ICIDS-IV has requirements for Department of the Army (DA) Technical Manuals (TMs). The Contractor shall comply with the manual requirements as set forth in Attachment A for development and production of equipment publications.

3.6 Training

ICIDS-IV site training will be a combination of classroom and hands-on training, utilizing Contractor installed ICIDS-IV equipment. Site training shall consist of an Operator, System Administrator, and Maintenance course. The Operator, System Administrator, and Maintenance training course shall be tailored to each installation according to the type and quantity of ICIDS-IV equipment being installed. In addition, an executive training course overview, for Program Office personnel, shall provide an outline of all ICIDS-IV training, and shall be presented at the contractor's facility. The Contractor shall comply with the training requirements as stated below and award a training certificate to each attendee upon completion.

3.6.1 General.

The Contractor shall develop a training package and conduct training for the ICIDS-IV in accordance with (IAW) the Statement of Work (SOW) and Contract Data Requirements List (CDRLs) A031, A032, and A033.

3.6.2 Requirements. The Contractor shall provide ICIDS-IV training as described below:

a. Government Executive Overview:

A one, 8 hour day Executive Training Course Overview at the Contractors established IDS test and evaluation laboratory, outlining all ICIDS-IV training, shall be provided for Program Office personnel prior to start of PVT-1. Additional course shall be offered as required upon request of the government.

b. Installation Training:

This is a block of instruction for Operators, System Administrators, and Maintenance Personnel that shall be provided at each ICIDS-IV installation. Operators must complete only the Operator portion of the training, while the System Administrators must complete the Operator portion of the course before taking the System Administrator training. The maintenance personnel will receive Operator and System Administrator training prior to learning the maintenance tasks. The course shall

be structured for classroom and hands-on training, utilizing installed ICIDS-IV equipment and shall include all operations and functions of the ICIDS-IV system to include Operator Preventive Maintenance Checks and Services (PMCS) for the ICIDS-IV equipment. All training shall be tailored for each installed site.

c. Training, Testing Materials, and Equipment.

The Contractor shall develop and provide all training, testing materials, and equipment for a 12-person class located at the Government site location IAW applicable CDRLs. These materials may include, but are not limited to: manufacturer's (commercial) manuals, ICIDS-IV technical manuals (TMs) as well as outlines, instructor guides, trainee guides, wall charts, schematics, video tapes, or films. All training and testing material developed shall be approved by the Government seven (7) workdays prior to contractor conducting the class. Upon approval, the Contractor shall provide each student at the installation site a copy of all training material developed and approved for the installation site.

d. Conduct of Courses.

(1) Course Objective. The Contractor shall conduct a training course on all operational and maintenance related actions for the ICIDS-IV system. The objective of the Operator, System Administrator, and Maintainer training courses are to ensure that each Operator can accomplish all of the operational actions and that each System Administrator can accomplish all of the operational actions and PMCS functions specified in the Operator and System Administrator sections of the technical manual. The maintenance training shall allow for the installation maintenance personnel to identify, remove, and replace failed major components of the system.

(2) Scope of Training. The training shall be a combination of classroom and hands-on (practical exercise) using the installed ICIDS-IV system. At the completion of each course, students will be given a test to assess knowledge gained during the program of instruction. System Operators will be tested on their ability to successfully accomplish all of the operational actions, System Administrators will be evaluated on their ability to accomplish all of the operational actions and PMCS functions and finally, System Maintainers will be tested on their ability to identify, remove, replace and perform prescribed maintenance of major components specified in the system technical manual.

(3) Length of Course. The Operator, System Administrator, and Maintenance courses shall not exceed 80 hours, and shall cover the ICIDS-IV delivered under this contract.

(4) Dates of Site Classes. Dates for presentation of each class will be determined by the Government, based on the site installation schedule, and the availability of installed ICIDS-IV equipment to be used for the training. Training shall be conducted at each ICIDS-IV installation.

(5) Safety. The Contractor shall establish detailed procedures, also included in the training material, to ensure the safety of all individuals concerned with the training

program. Safety procedures shall include relevant notices, warnings, cautions and notes extracted from the TMs (both commercial and military) and from any other source of information pertinent to the safety of personnel while in the training course.

(6) Facilities. Classroom and practical exercise/laboratory facilities will be furnished by the SPOC who will coordinate to ensure availability and adequate facility for the site training. All training will be given in an area free of interference from other classes or activities disruptive to a satisfactory training environment.

(7) Training Material. All training materials shall be furnished by the Contractor.

(8) Instructor Qualifications. The instructor(s), selected by the Contractor will be experienced and have a complete knowledge of the end item and all its components.

3.6.3 Special Instructions:

a. The Government reserves the right to record any or all training, photographically or electronically, for instructional use or review. Such material becomes the sole property of the Government and no additional copyright or individual release shall be required.

b. All visual aids/materials and test packages developed or specifically produced/manufactured for use in the conduct of training courses shall become the property of the Government upon completion of the training courses.

3.7 Warranty

A one-year warranty, including all parts and labor for all supplies delivered under this contract, is required (see Warranty provision in Section H). The Contractor shall provide warranty service 24 hours per day, 7 days per week. Maintenance Service reports detailing maintenance problem(s) and corrective action(s) taken shall be submitted IAW CDRL A010

3.7.1 Warranty Repair

The Contractor shall plan for repair actions on all items that fail during the one-year warranty. Specific tasks to be performed shall be addressed in the Contractor developed Maintenance Support Plan for each site IAW CDRL A009. This shall include repair, replacement, modification, test, and subsequent documentation of failed Contractor installed ICIDS-IV equipment. The Contractor shall provide a time line identifying when scheduled warranty maintenance will be performed at each site.

3.7.2 Warranty Repair Time

The contractor maintenance shall minimize interruptions of system operation not to exceed 24 hours. Repair time for unscheduled warranty repair of an operational mission failure shall not exceed the time specified (either 8 or 24 hours) in the delivery order. An operational mission failure is defined as any malfunction of the system that results in the loss of the ability of the equipment to perform its intended function, which would require the deployment of a guard force to 1/16th or greater of the protected zones. For other failures, the response and repair time shall not exceed 24 hours. Warranty Repair Time for service calls is measured from the time the Contractor is notified; to the time the Contractor’s work force has completed the repair.

3.8 Security.

In concert with FAR clause 52.204-2 (8/96), Security Requirements, the Contractor shall comply with the security regulations and procedures set forth in the National Industrial Security Program Operating Manual (NISPOM) and DD Form 254, Contract Security Classification Guide. Before performing and upon completion of any on-site work, the Contractor shall report to the Installation Security Officer or the designated representative. Contractor personnel shall possess and transmit appropriate clearances prior to arrival at the site. Pursuant to AR 190-11 and AR 190-13, Contractor personnel whose duties involve the design, operation, test, installation, or maintenance of unclassified IDS require completion of a favorable National Agency Check (NAC) or NAC with written inquiries prior to appointment to such non-critical, sensitive positions.

3.9 Configuration Control

3.9.1 Requirements

The Contractor shall be responsible for the configuration control of the ICIDS-IV hardware, COTS software, and interfaces as determined by the Performance Specification and verified during PVT. The Contractor shall utilize its internal plan to control the configurations of the ICIDS-IV components, control procedures for processing and recording changes to the configuration, and designate a configuration manager within its organization responsible for such changes. The initial configuration shall consist of the components as identified in the Schedule of Supplies or Services and Prices listed in Section B of the contract. All recommended changes to the ICIDS-IV system require prior approval, in writing IAW CDRL's A007 and A011, by the Contracting Officer. Any request for change shall be accomplished with complete supporting documentation, including the need or reason for change, and the price/schedule impact. If a reoccurring need is identified for a specific hardware and software item, the Contractor shall recommend that the Government incorporate the item into the contract. The Government reserves the right to require the Contractor to provide additional supporting technical analysis, and also reserves the right to specify additional testing as may be necessary to prove the acceptability of any proposed change prior to approval. The price of generated configuration changes, other than hardware upgrades or those requested by the Government shall be borne by the Contractor.

3.9.2 Hardware and Software Upgrades

The Contractor shall offer to the Government all hardware and software upgrades that are commercially available, which enable previously fielded products purchased under this contract to exhibit added performance, increased functionality and price option analysis. The Contractor shall notify the Contracting Officer within 60 days of product availability, and indicate if the old configuration will no longer be supportable. Commercial Drawings and Associated Lists for such hardware upgrades shall be furnished IAW CDRL A011. Documentation for such software upgrades shall be furnished IAW CDRL A007.

4.0 QUALITY ASSURANCE REQUIREMENTS

4.1 Responsibility for Inspection

Unless otherwise specified in the contract, the Contractor is responsible for the performance of inspection requirements. The Contractor shall provide and maintain an inspection system that shall assure that all supplies and services submitted to the Government for acceptance conform to contract requirements, whether manufactured or procured by the Contractor, or procured from subcontractors or vendors. The Contractor shall perform or have performed the inspections and tests required to substantiate product conformance to drawings, specifications, and contract requirements, and shall also perform all inspections and tests otherwise required by the contract. The Contractor's inspection system shall be documented and shall be available for review by the Government throughout the life of the contract.

4.2 Test and Evaluation

4.2.1 General

The Contractor shall perform tests as described in the following paragraphs. The Contractor shall provide personnel, equipment, instrumentation, and supplies necessary to perform all testing, unless otherwise indicated.

4.2.2 Performance Verification Test (PVT)

Government acceptance of the first system installed shall not take place until Government approval of all test reports submitted in support of PVT, which will consist of Performance Verification Testing (PVT) and an Endurance Test.

4.2.2.1 PVT-1

a. General. The Contractor shall conduct PVT in two (2) parts as described below. PVT-1 shall be conducted IAW the Contractor-prepared and Government-approved Test Plan (CDRL A012) and Test Procedure (CDRL A013) to verify all functional requirements of the ICIDS-IV, as set forth in the contract. These laboratory tests shall be conducted at the Contractor’s facility. The Test Report shall be submitted IAW CDRL A014.

b. PVT-1. PVT-1 shall be conducted on a fully integrated system consisting of at least one component of each hardware/software item except exterior sensors. The Contractor shall conduct tests to verify that system performance complies with contract requirements, IAW approved test plans and procedures. Model numbers of equipment tested shall be identical to those to be delivered.

4.2.2.2 PVT-2 and Endurance Test

a. General. The PVT-2 Test shall not be started until PVT-1 has been conducted and approved by the Government. Prior to conducting testing, the Contractor shall submit a Safety Assessment Report IAW CDRL A015. PVT-2 and an Endurance Test shall be conducted on the first site installed. Those components to be installed shall be new units. At least one component of each installed hardware/software item shall be tested or results from previous testing may be provided to the

Government for evaluation and approval. The Contractor shall prepare, for Government approval, PVT-2 and Endurance Test Plans, IAW CDRLs A016 and A019 respectively, and Test Procedures, IAW CDRLs A017 and A020, respectively. Upon completion of testing, the Contractor shall submit the PVT-2 and Endurance Test Reports, IAW CDRLs A018 and A021, respectively. The Contractor shall not be held responsible for failures in system performance resulting from the following:

(1) An outage of the main power supply in excess of the capability of any backup power source, provided that the automatic initiation of all backup sources and automatic shutdown and restart of the ICIDS-IV were accomplished.

(2) Failure of a Government furnished communications link, provided that the failure was not due to contractor-furnished equipment, installation, or software.

(3) Failure of existing Government owned equipment, provided that the failure was not due to contractor-furnished equipment, installation, or software.

(4) Failures due to environmental extremes exceeding the ICIDS-IV specification characteristics.

b. PVT-2. The Contractor shall verify that the completed ICIDS-IV complies with the contract requirements. PVT-2 shall verify successful system integration at the site, and shall verify proper installation of the system. Using approved test procedures, all physical and functional requirements of the ICIDS-IV shall be verified and documented. The Contractor shall make final adjustments and test all equipment, verify Data Transmission Media (DTM) operation, place the integrated system in service, and test the integrated system. The Government may terminate testing at any time when the system fails to perform as specified in the contract. Upon termination of testing, the contractor shall commence an assessment period. During the assessment period, the contractor shall identify all failures, determine the causes of all failures, correct all failures, and deliver to the Government a written report IAW CDRL A022. The report shall explain in detail the nature of each failure, corrective action taken, results of tests performed, and shall recommend the point at which testing should be resumed. After delivering the written report, the Contractor shall convene a test review meeting at the job site to present the results and recommendations to the Government. Based on the Contractor's report and the test review meeting, the Government will approve a restart date, or may require that testing be repeated. The price of any restarts or repeats shall be borne by the Contractor. Upon successful completion of the PVT-2 part of PVT, the contractor shall deliver a test report, IAW CDRL A018, to the Government prior to commencing the Endurance Test.

c. Endurance Test. The Endurance Test shall be conducted as specified below, and shall not be started until the Government approves the PVT-2 part, training has been completed, and all outstanding deficiencies have been corrected. The Contractor shall provide personnel to support the test 24 hours per day, including weekends and holidays, during the 30-day endurance test. The Government shall operate the system during this test. The test shall demonstrate that the system operates as specified. Test plans, procedures, and reports shall be IAW the data items identified in Paragraph 4.2.2.2a, above. The Contractor shall make no repairs during this part of testing unless authorized by Government Test Director. The Government may terminate testing at any time the system fails to perform as specified in the contract. Upon termination of testing by the Government,

the Contractor shall commence an assessment period as described in Paragraph 4.2.2.2b, above. The price of all retests shall be borne by the Contractor.

4.2.2.3 Supportability

Contractor shall implement reliability and maintainability programs to assure reliability requirements of the ICIDS-IV performance specifications are met.

The Contractor shall identify all failures, determine the causes of all failures, correct all failures, and deliver to the Government a written report IAW CDRL A023.

4.2.3 Test Readiness Review

a A Test Readiness Review (TRR) shall be conducted by Government prior to any test.

b. The Contractor is responsible for attending meeting and providing the required documentation and assistance in the resolution of any issues or concerns.

c. Discrepancies in the documentation, design, or training will be corrected prior to the conduct of the PVT and the Endurance Test by the Contract Site Manager, and may involve re-test of zones and re-training of personnel at contractor's expense.

4.2.3.1 During the course of PVT-2 and subsequent System Performance Verification (SPV) tests, all installed equipment shall be activated and report to the head end command & control console. The SPV test shall be conducted in such a manner that 100% of installed devices shall be activated.

4.2.4 System Acceptance Test (System Performance Verification [SPV] and Endurance Test)

The Contractor shall conduct a System Performance Verification (SPV) test, for follow-on site installations. After completion of the SPV, the Government shall conduct a thirty (30) day Endurance Test, as described in Paragraph 4.2.2.2 c. above. Test Plans shall be IAW CDRLs A024 and A027, respectively. Test Procedures shall be IAW CDRLS A025 and A028, respectively. Test Reports shall be IAW CDRLs A026 and A029, respectively. When agreed to between the Government and the Contractor, the scope of the testing required may be tailored to address site specific requirements.

4.2.5 The contractor shall provide certified personnel for the installation, maintenance, training, and administration of all ICIDS-IV Original Equipment Manufacturer (OEM) equipment.

4.2.6 The contractor shall ensure that the ICIDS-IV is in compliance with Department of Defense Instruction (DODI) 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997, **DoD Directive (DoDD) 8500.1, DoD Directive (DoDD) 8500.2, DoD Instruction (DoDI) 8500.1, DoD Instruction (DoDI) 8580.1, DoD 8510-1M.** The system shall be certified/accredited prior to First Unit Equipped (FUE).

SECTION L,
INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

L.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998) (Reference 52.107(a))

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full Text. Upon request, the Contracting Officer will make their full text available. The Offeror is cautioned that the listed provisions may include blocks that must be completed by the Offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the Offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at these addresses:

http://www.arnet.gov/far
http://farsite.hill.af.mil
http://www.acq.osd.mil/dpap/dars/dfars/index.htm

(End of provision)

L.2 52.204-7 Central Contractor Registration (Oct 2003) (Reference 4.1104).

L.3 52.211-6 BRAND NAME OR EQUAL (AUG 1999) (Reference FAR 11.107(a))

L.4 52.211-2 Availability of Specifications, Standards, and Data Item Descriptions Listed in the Acquisition Streamlining and Standardization Information System (ASSIST) (Jan 2006) (Reference 11.204(b)

(End of provision)

L.5 52.211-14 NOTICE OF PRIORITY RATING FOR NATIONAL DEFENSE USE (SEP 1990) Reference 11.604(a))

Any contract awarded as a result of this solicitation will be /_/ DX rated order; /X/ DO rated order certified for national defense use under the Defense Priorities and Allocations System (DPAS) (15 CFR 700), and the Contractor will be required to follow all of the requirements of this regulation.

(End of provision)

L.6 52.215-1 INSTRUCTIONS TO OFFERORS--COMPETITIVE ACQUISITION (Jan 2004)--ALTERNATE I (OCT 1997) (Reference 15.209(a) (1)

L.7 52.216-1 TYPE OF CONTRACT (APR 1984) (Reference 16.105)

Based on the Governments (vast) 24 years experience with ICIDS since 1992, a FFP type contract with some T&M elements is contemplated. If alternatives are recommended the potential offeror must address the applicability and rationale provided at part 16 of the FAR and 216 of the DFARS, and must comment on the relevant risk factors for the Government to consider alternative contract types.

(End of provision)

L.8 52.222-24 PREAWARD ON-SITE EQUAL OPPORTUNITY COMPLIANCE REVIEW (FEB 1999) (Reference 22.810(c))

L.9 52.233-2 SERVICE OF PROTEST (AUG 1996) (Reference 33.106(a))

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the General Accounting Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from the following person:

Ms. Lynn Selfridge
U.S. Army Space and Missile Defense Command
64 Thomas Johnson Drive
Fredrick, MD 21702

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of provision)

L.10 252.204.7004 REQUIRED CENTRAL CONTRACTOR REGISTRATION (NOV 2003) (Reference 204.1104)

L.11 ALTERNATE PROPOSALS

Alternate proposals/solutions will not be considered.

L.12 ACKNOWLEDGEMENT OF SOLICITATION AMENDMENT

Should an amendment be issued against this solicitation, the Offeror shall acknowledge, by signing the Standard Form (SF) 30 entitled Amendment of Solicitation/Modification of Contract, and include it in the proposal submission.

L.13 SOLICITATION DISTRIBUTION

(a) No paper distribution of this solicitation will be made. The solicitation, all amendments, and other information will be made available on the US Army Space and Missile Defense (USASMDC) Web Site:

http://www.smdc.army.mil/Contracts/Contracts.html

However, it is highly advisable to provide an e-mail address and point of contact as the Government may resort to e-mailing in the event of unforeseen system failures. Requests to be placed on the mailing list may be sent to:

Mr. Greg Florey at: greg.florey@det.amedd.army.mil

Please be sure to include your company name, address, point of contact, e-mail address, and telephone number in your request.

L.14 PROPOSAL PREPARATION INSTRUCTIONS

L.14.1 These instructions prescribe the format for the proposal and describe the approach for the preparation and presentation of the proposal data. They are designed to ensure that the Offerors submit the required information essential to the Government's understanding and validation of their proposals. Offerors are cautioned and encouraged to follow these instructions completely and carefully.

L.14.2 Proposal Submission Address. Submit signed and dated offers to the following address:

Ms. Lynn Selfridge
U.S. Army Space and Missile Defense Command
64 Thomas Johnson Drive
Fredrick, MD 21702

L.14.2.1 Proposal Due Date/Time: 11:00 a.m., *EST, XXX XX*, 2006. Proposals received at the above address after the time and date specified for receipt will be considered LATE in accordance with FAR 52.215-1 Instructions to Offerors – Competitive Acquisition located at L.6, above.

L.14.2.2 Hand delivered proposals: Proposals may be accepted between the hours of 8:00a.m., EST and 4:30 p.m., EST, Monday through Friday at the address listed above.

L.14.3 Proposal Format

Each proposal shall be submitted in separate volumes as outlined below in both hardcopy and electronic form as described below.

Volume/Part	Subject (Page limitations)	Copies Hard/electronic
Volume I	Technical Proposal	3/3
Part I	Executive Summary & Management Approach (5 pgs)	3/3
Part II	Technical – System Design (300 pgs)	3/3
Part III	Technical – System Installation (50 pgs)	3/3
Part IV	Technical – System Demonstration (50 pgs)	3/3
Part V	Technical – System Supportability (25 pgs)	3/3
Part VI	Technical Exceptions (5 pgs)	3/3
Volume II	Cost/Price Proposal	3/3
Part I	Completed Cost/Price Model (25 pgs plus spreadsheet)	3/3
Part II	Completed Section B (Priced CLIN List)(final #)	3/3
Volume III	Past Performance (50 pgs)	3/3
Volume IV	Contract Proposal (50 pgs)	1/1
Part I	Standard Form (SF) 33, Solicitation, Offer, and Award	1/1
Part II	Section K, Representations and Certifications	1/1
Part III	Vendor Agreements	1/1
Part IV	Subcontracting Plan	1/1
Part V	Business Exceptions	1/1

TABLE 1

L.14.4 Page Format Requirements.

L.14.4.1 The following parameters are established for the printed page:

Page Size	8-1/2" X 11"
Text Line per Page	No more than 58
No. of Spaces Top Margin	2
Default Pitch	5 = (12 characters/inch)
Spacing	Single Spacing
Page Count Restriction	See above table for page limit
Header or Footer Marking -- Identification	RFP Number
Header or Footing Marking -- Proprietary Data	See FAR 52.215-1

L.14.4.2 Electronic Format Requirements.

Note: ELECTRONIC FILES SHALL NOT BE IN ZIP FILE FORMAT.

The following parameters are established:

Volume I: CD/ROM IN MS WORD OR PDF SEARCHABLE TEXT FORMAT.

Volume II: Price Model – CD/ROM in Microsoft Excel, Version 5.0 or later (delete "macros" before submittal); Priced Section B – CD/ROM shall be in MS Word or PDF Searchable Text Format. The electronic spreadsheets shall not be compiled or password protected. All cells and formulas shall be visible, editable, and unprotected. Offerors shall not establish links within these files.

Volumes III - IV: CD/ROM IN MS WORD OR PDF SEARCHABLE TEXT FORMAT. A directory listing of the CD/ROMs shall accompany the proposal with a listing of file names according to table 1 above and the contents of each file. (Attach directory to proposal transmittal letter.)

NOTE. The content of the electronic copies of the Offeror's proposal must be identical to the hard-copy proposal submitted in response to this RFP. The Government is not responsible for identifying inconsistencies between the two and may rely on either version at its discretion.

NOTE. To prevent the spread of virus that can damage documents, Microsoft Word and Excel Offeror proposal documents shall not contain any "macros" or hyperlinks.

L.14.5 Proposal Volume Contents.

All information shall be confined to the appropriate part of each volume of the proposal; that is, no cross-referencing between volumes is permitted.

At the front of Part II of Volume I, Technical Proposal, the Offeror shall include 1) a "Proposal-to-Statement of Work (SOW)" cross-reference matrix that indicates the SOW requirement (or Section L) paragraph that is being addressed by the indicated proposal paragraph, and 2) a separate "Proposal-to-Specification" cross-reference matrix that indicates if the proposal **Meets** or **Exceeds** each paragraph and subparagraph of paragraphs 3, 4, 5, and 6 of the ICIDS System Specifications ICIDS-PS-0600, ICIDS-PS-0601, and ICIDS-PS-602.

<u>All information that the offerors wants the Government to evaluate shall be included in its proposal submission.</u>

L.14.5.1 Volume I – Technical Proposal.

.

L.14.5.1.1 Technical Proposal Instructions - General

Proposals which merely offer to conduct a program in accordance with the

requirements of the Government's statement of work or merely reiterates the Governments instructions shall not be considered to have met the minimum requirements for any factor/subfactor/element set forth in section M of this RFP.

A. A detailed work plan must be submitted indicating how each aspect of the statement of work is to be accomplished. The technical proposal should reflect a clear understanding of the nature of the work being undertaken.

B. The technical proposal must include information on how the project is to be organized, staffed, and managed. Information should be provided which will demonstrate your understanding and management of important events or tasks. You must explain how the management and coordination of consultant and/or subcontractor efforts will be accomplished.

C. The technical proposal must contain a discussion of present or proposed facilities and equipment which will be used in the performance of the contract.

D. Any offered technology will be unencumbered by any intellectual property protection or that the offeror has the legal right to provide the offered technology.

L.14.5.1.2 Part I – Executive Summary & Management Approach

A. The Executive Summary will include an introduction and a summary of Volumes I, III, IV.

B. The Offeror shall discuss completely and in detail its proposed approach for mitigating the management of the ICIDS-IV system design, system installation, system demonstration, and system supportability.

C. The Offeror shall include an organizational chart listing the titles and proposed duties of the key personnel, consultants, and key subcontractor employees assigned to the project. Their resumes shall be included and should contain information on education, background, recent experience, and specific scientific or technical accomplishments.

D. Corporate Management Experience and Expertise. The Offeror shall discuss its corporate management experience with the programs identified in Volume III that are similar to ICIDS-IV:

1) in value, scope, and complexity;

2) the qualifications, education, experience and availability of key management personnel for their roles under the proposed effort; and

3) its procedures for implementing lessons-learned throughout the corporation.

L.14.5.1.3 Part II – Technical – System Design

Note: All hardware and software/firmware offered must be currently commercially available.

A. The Offeror shall provide the following information for each component offered:

1) make and model of the component(s) proposed and a specification sheet for each proposed component;

2) a brief description of the component(s); and

3) a concise explanation of the differences between the Performance Equivalence Sheets and the equipment proposed.

B. The Offeror shall provide a complete and detailed technical description of its proposed ICIDS-IV system design. It shall include the following:

1) The Offeror shall describe, in detail, its technical approach and overall ability to perform Site Survey/Site Specific Design (SSD).The proposal shall address design standards; computer aided design/drafting utilization; design drawings/diagrams; design analysis; site preparation and installation plan; communications media testing and certification; and identification of site preparation requirements; and labor categories, hours, schedule and parts list.

2) the anticipated performance of the proposed system architecture, including interfaces, design, communications (to include each communication link, number of transmission lines, transmission protocol, encryption protocol method and data rates required in each link), and components comprising the proposed system;

3) identification of the proposed system and application software, to include identification of the operating system and required support software;

4) proposed features of the system software;

5) proposed approach to Quality Assurance;

6) proposed method of control for the ICIDS-IV configuration baseline pertaining to system components and various interfaces;

7) proposed primary power certification and system power requirements;

8) proposed communications media testing and system communication requirements;

9) proposed method for adding to, removal of, or enhancing the existing Intrusion Detection System (IDS);

10) proposed method for adding to, removal of, or enhancing the Existing Entry Control Equipment (ECE);

11) proposed method for adding to, removal of, or enhancing the Closed Circuit Television (CCTV) used for intrusion assessment;

12) perform a Gap Analysis to ensure the design meets regulatory compliance;

13) proposed method for achieving system accreditation IAW DoD Information Technology Security Certification and Accreditation Process (DITSCAP);

14) proposed method to handle advances in technology and to incorporate those changes into ICIDS-IV;

15) proposed process to handle the obsolescence of proposed ICIDS-IV equipment;

16) proposed approach to provide technical manuals prepared in accordance with Attachment A (Requirements for Development and Production of Equipment Publications) to the SOW for ICIDS-IV; and

17) proposed approach to provide the operator, system administrator, and maintainer training courses prior to installation of the ICIDS-IV system.

C. The offeror shall provide a complete and detailed design, drawings, labor categories and hours, schedule, and parts list for the site survey and design, phases for the attached pseudo-site “Fort FPS” (Attachment x). The pseudo-site will be one of the primary elements utilized by the Government to evaluate the offerors technical and cost approach for contract award.

L.14.5.1.4 Part III - Technical – System Installation.

A. The Offeror shall provide a complete and detailed technical description of its proposed ICIDS-IV system installation. It shall also include the following:

1) the ability to obtain and retain personnel capable of obtaining a favorable National Agency Check (NAC) clearance prior to beginning work on any delivery order;

2) proposed method of qualifying (diploma, certifications, licenses, skill set, experience installing similar commercial security systems, etc…) the Program Manager, Site Managers, Engineers, Technicians, Electricians, Quality Control and Configuration Management;

3) process whereby workmanship will meet quality assurance and quality control in accordance with offerors quality assurance plan;

4) process of equipment and material management control from purchasing through installation;

5) disposal methods for de-installed equipment and refuse; and

6) description of Offerors understanding of best commercial standards and practices with respect to an IDS as specified in the Performance Specifications and UL-1076.

B. The Offeror shall provide a complete and detailed description of its proposed ICIDS-IV system installation method of coordination and communications with the various organizations (PM-FPS, Contracting Agency, Site POCs and tenant activity POCs) to ensure a successful project.

C. The offeror shall provide a complete and detailed design, drawings, labor categories and hours, schedule, and parts list for the installation phase for the attached pseudo-site "Fort FPS" (Attachment x).

L.14.5.1.5 Part IV - Technical – System Demonstration.

A. The Offeror shall provide a complete and detailed technical description of its proposed ICIDS-IV system demonstration IAW SOW Section 4.2, Test and Evaluation. Additionally, it shall include the following:

1) regression analysis testing approach and change control IAW SOW Section 3.9.1 Configuration Control;

2) the proposed Performance Verification Test (PVT-1) in the laboratory environment;

3) location of laboratory for Performance Verification Test (PVT-1) and follow on testing and evaluation IAW SOW Paragraph 3.3.b.

4) method of supporting and maintaining laboratory operation IAW SOW Paragraph 3.3.b.

5) the proposed Performance Verification Test (PVT-2) and Endurance Test for the first installed site and System Acceptance Test (System Performance Verification and Endurance Test) for follow-on sites;

6) method of documenting test and evaluation data IAW CDRLs A014, A021, A022, A026, A029.

B. The offeror shall provide a complete and detailed design, drawings, labor categories and hours, schedule, and parts list for the installation phase for the attached pseudo-site "Fort FPS" (Attachment x).

L.14.3.1.5 Part V - Technical – System Supportability.

A. The Offeror shall provide a complete and detailed technical description of its proposed ICIDS-IV system supportability plans. It shall also include the following:

1) methods of managing and validating system software/hardware configuration change control/version control IAW SOW Section 3.9.1, Configuration Control;

2) procedures for problem reporting and warranty issues;

3) describe Help Desk availability, functions, and procedures;

4) warranty maintenance plan and implementation IAW SOW Paragraph 3.7 and CDRL A010; and

5) system backup to include recovery management planning, documentation and procedures.

B. The offeror shall provide a complete and detailed design, drawings, labor categories and hours, schedule, and parts list for the warranty phase for the attached pseudo-site "Fort FPS" (Attachment x).

L.14.5.1.7 Part VI – Technical Exceptions.

Any exceptions to the SOW, Attachment A (Requirements for Development and Production of Equipment Publications), or Performance Specifications technical requirements shall be addressed at this tab. The Offeror shall clearly identify the paragraph and the requirement to which the exception is being made and include appropriate supporting rationale for each exception.

L.14.5.2 Volume II – Cost/Price Proposal. Based on the input received from the Draft RFP responses and the final decision of contract type/CLIN structure, instructions regarding the price proposal/Section B may change from that shown below.

Offerors shall structure their proposal to satisfy the requirements of the Performance Specifications, Attachments, and SOW while following the format outlined below, paragraph by paragraph. In addition, the Offeror shall provide pricing for the proposed sample "Fort FPS" site survey, site specific design, and installation to include parts, labor, and travel.

L.14.5.2.1 Part I – Cost/Price Model.

L.14.5.2.1.1 Offerors are cautioned to read the Cost/Price Model instructions located at Section J, Attachment 9 of the solicitation. The CostPrice Model is password protected in all of the appropriate areas. However, Offerors are cautioned not to tamper with the formulas in any way. Offerors are reminded that its submissions must not be password protected.

L.14.5.2.1.2 To assist the Offeror in completing the Cost/Price Model, the anticipated award date is 1stQTR FY07.

L.14.5.2.1.3 Quantities listed in the Cost/Price Model are for evaluation purposes only; quantities are estimates and do not necessarily reflect the quantities to be procured after contract award.

L.14.5.2.1.4 Except as specifically authorized by the solicitation all CLINs shall be priced and shall be separately orderable. The Government reserves the right to reserve any CLIN on the contract at any time throughout the ordering period. Accordingly, pricing for any CLIN must stand alone, and not be dependent upon authorization of any other CLIN. The only SLIN to be "Not Separately Priced" (NSP) is, CDRL A001 Monthly Management Report. No CLINs are to be proposed as NSP.

L.14.5.2.1.5 Offerors are cautioned not to insert additional or optional CLINs or SLINs, or change the formulas in the Cost/Price Model file in any way, without prior written authorization of the Contracting Officer. Offerors' electronic submission must not be linked or password protected.

L.14.5.2.1.6 This is an Indefinite Delivery Indefinite Quantity (IDIQ) contract, and estimated quantities are noted by contract year in the Cost/Price Model. Quantity or volume price discounts, where pricing is contingent upon certain ordering limits being achieved, will not be considered for award purposes.

L.14.5.2.1.7 The Cost/Price Model shall be in MS EXCEL 2003, format for both hardcopy and digital media.

L.14.5.2.2 Part II -- Section B (Priced CLIN List).

Section B (Priced CLIN List) shall be priced in accordance with the instructions contained in Section B. Offerors shall submit Section B on the same Digital Media as the Cost/Price Model (room permitting) in either Windows XP/*Word* 2003 for both hardcopy and Digital Media.

L.14.5.3 Volume III – Past Performance

L.14.5.3.1 The Offeror shall identify not more than five (5) relevant Government and/or commercial contracts (prime or first-tier subcontracts) which it has performed during the past

three (3) years. To be relevant, these contracts must be for efforts that have a logical connection with the effort required by the ICIDS-IV solicitation. This volume shall be organized as follows:

A. Contract Descriptions. The description of each contract and subcontract shall include the following information in the order listed:

(1) Contractor place of performance, CAGE Code and DUNS number.

(2) Government/Commercial Contracting activity, address, telephone and FAX numbers, and email address.

(3) Procuring Contracting Officer's name, telephone and FAX numbers, and email address.

(4) Government/Commercial Technical Representative/COR, telephone and FAX numbers, and email address.

(5) Government contract administration activity, and the Administrative Contracting Officer's name, telephone and FAX numbers, and email address.

(6) Government contract administration activity's Pre-Award Monitor's name, telephone and FAX numbers, and email address.

(7) Contract number.

(8) Contract type.

(9) Awarded price.

(10) Final, or projected final price.

(11) Original delivery schedule.

(12) Final, or projected final delivery schedule.

(13) Provide information of the firm's safety record. Include information about:

a. on-the-job accidents
b. work days lost
c. OSHA violations
d. days worked without an accident

(14) Briefly describe the circumstances surrounding the following:

a. projects completed appreciably ahead of schedule; identify projects which had delays

b. contract termination in whole or in part and reason
c. projects in which damages were assessed against your firm

NOTE. The Offeror is responsible for verifying the email address of each Point of Contact (POC) by submitting an e-mail message to the addressee and verifying receipt of same by the addressee.

B. Technical Experience. Offerors shall provide a specific narrative explanation of each contract listed describing the objectives achieved and detailing how the effort is relevant to the requirements of this solicitation.

C. New Corporate Entities and Other Entities without Relevant Past Performance. These entities may submit the above data on contracts involving predecessor companies, if applicable.

L.14.5.3.2 Data Sources. Both independent data and data provided by Offerors in its proposals may be used to evaluate past performance. Since the Government may not necessarily interview all of the sources provided by the Offeror, the Offeror must explain the relevance of the data provided. The Government is not required to search for data to cure problems and risks it finds in proposals. The burden of providing complete, current, and relevant past performance information remains with the Offeror.

L.14.5.3.3 Past Performance Questionnaire.

Offerors shall complete the Contract Data section of the Questionnaire (located in Section J, Attachment X); submit the Letter and Questionnaire to all POCs identified in Volume III, Paragraph A; and request that the POCs complete the Questionnaire and return by fax at the following number or e-mail at the following address, NLT the proposal due date:

FAX: (301) 619-5609
greg.florey@det.amedd.army.mil

NOTE. The Questionnaire shall be faxed or e-mailed directly to the above; it shall not be returned to the Offeror.

L.14.5.4 Volume IV – Contract Proposal.

L.14.5.4.1 Part I – Standard Form (SF) 33, Solicitation, Offer, and Award.

This part shall contain a completed and signed copy of SF 33 and a signed copy of each amendment, if any, to the solicitation. Use in MS Word or PDF searchable text format. files for the electronic copy of the proposal.

L.14.5.4.2 Part II – Section K, Representations and Certifications.

This part shall contain a completed copy of Section K. Attach continuation pages at the end of Section K, if required to complete a response to a provision.

L.14.5.4.3 Part III – Vendor Agreements.

Offerors are advised that the commercial firm identified below will assist the Government in the evaluation process. The use of contractors to assist in the evaluation will be strictly controlled. This firm will be authorized access to only those portions of the proposal data and discussions that are necessary to enable them to perform their respective duties. They will have access to prices and labor rates in the price proposal, if required to assist the Price Team in its price analysis. The firm shall be expressly prohibited from competing on the subject acquisition.

FIRM: Computer Sciences Corporation
7405 Alban Station Court, Suite B-200
Springfield, VA 22150
Telephone: (703) 452-3708
Facsimile: (703) 912-6082

In accomplishing the duties related to the source selection process, the aforementioned firm may require access to proprietary information contained in the Offerors' proposals. Therefore, pursuant to FAR 9.505-4, this firm must execute a Vendors Agreement with each Offeror which states that they will (1) protect the Offeror's information from unauthorized use or disclosure for as long as it remains proprietary, and (2) refrain from using the information for any purpose other than that for which it was furnished.

It is the responsibility of each Offeror to contact the above firm and to take all reasonable steps that may be required to obtain the required FAR 9.505-4 agreement. To expedite the evaluation process, it is requested that each Offeror contact the above firm to effect execution of such agreement prior to submission of proposals. Each Offeror shall submit copies of the Vendors Agreements with their Contract Proposal.

For the purpose of executing this agreement with Computer Sciences Corporation, please contact:

Computer Sciences Corporation
Mr. Tom Clavin
Telephone: (703) 452-3708
Facsimile: (703) 912-6082

L.14.5.4.4 Part IV – Subcontracting Plan.

This part shall contain the Offeror's subcontracting strategy, to include all major subcontractors.

L.14.5.4.5 Part V – Business Exceptions/Alternatives (Terms and Conditions).

A. Offerors are cautioned that they take exception to any Terms and Conditions of the solicitation at their own risk. The Government may, at its option, reject an offer, which contains any such exceptions.

B. Nonetheless, any exception taken by the Offeror at its own risk shall be identified in this part. The Offeror should clearly identify the paragraph and term or condition to which the exception is being made and include appropriate supporting rationale for any exception.

C. Suggested, optional wording changes (to include clarifications and addenda) to any requirements of the solicitation shall be identified in this part. The Government may, at its option, accept or reject any such changes. If accepted, it may be necessary to amend the solicitation and to discuss the changes with other Offerors.

If no exceptions are taken, the Offeror shall include the following statement in this part of the proposal:

"[Name of Offeror] takes no exception to any requirements of Solicitation No. W9113M-06-R-0011, ICIDS-IV."

END OF SECTION L

SECTION M

EVALUATION FACTORS FOR AWARD

M.1 52.217-5 EVALUATION OF OPTIONS (JUL 1990) (Reference 17.208(c)(1))

M.2 BASIS FOR AWARD.

Any award to be made will be based on the best overall (i.e. Best Value) proposal that is determined to be the most beneficial to the Government, with appropriate consideration given to the three evaluation factors: Technical, Past Performance, Cost/Price.

To receive consideration for award, a rating of no less than "Acceptable" must be achieved for the Technical Factor, all Technical Subfactors and the Past Performance Factor. Offerors are cautioned that an award may not necessarily be made to the lowest evaluated cost, but whose technical and past performance proposals are significantly more advantageous to the government.

M.3 FACTORS AND SUBFACTORS TO BE EVALUATED.

M.3.1 EVALUATION FACTORS AND SUBFACTORS AND THEIR RELATIVE ORDER OF IMPORTANCE

Factor I – Technical.
- Subfactor A: System Design
- Subfactor B: System Installation
- Subfactor C: System Demonstration
- Subfactor D: System Supportability

Factor II – Past Performance

Factor III – Cost/Price

The Technical Factor is more important than the Past Performance Factor; the Past Performance Factor is more important than the Cost/Price Factor. Within the Technical Factor, the subfactors are listed in descending order of importance. All evaluation factors other than cost/price, when combined, are significantly more important than cost/price.

(a) Subfactor A – System Design. The Government evaluation will consist of a comprehensive assessment of the proposed ICIDS-IV Performance of the proposed system architecture, including interfaces, design, communications, and components of the proposed system; identification and detailed description and features of the proposed system and application software, to include operating system and support software; approach to Quality Assurance and configuration control; communications media testing and system communication requirements; methodology for adding to, removal of, or enhancing the existing Intrusion Detection System

(IDS); methodology for adding to, removal of, or enhancing the existing Entry Control Equipment (ECE); methodology for adding to, removal of, or enhancing the Closed Circuit Television (CCTV) used for assessment; Gap Analysis during Site Survey/Site Specific Design phase to ensure the design meets regulatory compliance; methodology for achieving system accreditation IAW DoD Information Technology Security Certification and Accreditation Process (DITSCAP); methodology for handling changes and/or advances in technology and implement those changes into ICIDS-IV; methodology for handling the obsolescence of proposed ICIDS-IV equipment over the potential life of the program (base plus out years); methodology for performing Site Survey/Site Specific Design (SS/SSD) including design standards, computer aided design/drafting utilization, site preparation and installation planning, communications media testing and identification of site preparation requirements; approach to technical manuals; and approach to operator, system administrator, and maintainer training courses prior to installation of the ICIDS-IV system; and technical approach, detailed design drawings, labor categories and hours, schedule, and parts list based on provided pseudo-site "Fort FPS" (Attachment X) for Site Survey/Site Specific Design.

(b) Subfactor B – System Installation. The Government evaluation will consist of a comprehensive assessment of the proposed ICIDS-IV personnel clearances; personnel qualification methods; workmanship evaluation and quality assurance; material tracking; disposal methods for de-installed equipment and refuse; understanding of best commercial standards; method of coordination and communications with the various organizations (PM-FPS, Contracting Agency, Site POCs and tenant activity POCs) to ensure a successful project; and technical approach, detailed design drawings, labor categories and hours, schedule, and parts list based on provided pseudo-site "Fort FPS" (Attachment X) for System Installation.

(c) Subfactor C – System Demonstration. The Government evaluation will consist of a comprehensive assessment of the proposed ICIDS-IV the proposed Performance Verification Test-1 (PVT-1) in the laboratory environment; location of laboratory for PVT-1; method of supporting and maintaining laboratory operation throughout the life of the ICIDS-IV contract; the proposed Performance Verification Test (PVT-2) and Endurance Test for the first installed site; the proposed System Acceptance Test (SPV and Endurance Test) for follow-on sites; methods of documenting test and evaluation data IAW CDRLs A014, A021, A022, A026, and A029; regression analysis/test approach; change control; and technical approach, detailed design drawings, labor categories and hours, schedule, and parts list based on provided pseudo-site "Fort FPS" (Attachment X) for System Demonstration.

(d) Subfactor D – System Supportability. The Government evaluation will consist of a comprehensive assessment of the proposed ICIDS-IV methods for managing and validating system software/hardware configuration control; procedures for problem reporting and warranty issues; Help Desk plans and procedures; warranty maintenance planning; system backup and recovery management planning, documentation and procedures; and technical approach, detailed design drawings, labor categories and hours, schedule, and parts list based on provided pseudo-site "Fort FPS" (Attachment X) for System Supportability.

M.3.2 Factor II – Past Performance Factor: No subfactors.

M.3.3 Factor III – Cost/Price Factor: No subfactors.

M.4 EVALUATION APPROACH.

M.4.1 All proposals shall be subject to evaluation by a team of Government personnel and non-Government advisors from the following company: Computer Sciences Corporation

M.4.2 Technical Evaluation Approach. The evaluation process will consider the following for each subfactor, as applicable and except as otherwise noted:

(a) Understanding of the Problems. The proposal will be evaluated to determine the extent to which it demonstrates a clear understanding of all features involved in solving the problems and meeting the requirements; and the extent to which uncertainties are identified and resolutions proposed.

(b) Feasibility of Approach. The proposal will be evaluated to determine the extent to which the proposed approach is workable and the end results achievable. The proposal will be evaluated to determine the extent to which successful performance is contingent upon proven devices and techniques that do not require development. The proposal will be evaluated to determine whether the offeror's methods and approach in meeting the requirements in a timely manner provide the Government with a high level of confidence of successful completion. The proposal will be evaluated to determine the extent to which the offeror is expected to be able to successfully complete the proposed tasks and technical requirements within the required schedule.

(c) Flexibility. The proposal will be evaluated to determine the extent to which the approach facilitates the implementation of both cost effective and simplified integration of new processes and technology enhancements, and unanticipated future changes to the overall system.

(d) Completeness. Each proposal will be rated strictly in accordance with its written content based on the extent to which requirements have been considered, defined and satisfied. **Evaluators will not assume that the Offeror's performance will include areas not specified in its proposal.**

M.4.3 Past Performance Evaluation Approach. The Past Performance evaluation will assess the relative risks associated with an offeror's likelihood of success in performing the solicitation's requirements as indicated by that offeror's relative record of past performance. In this context, "offeror" refers to the proposed prime contractor and all proposed major subcontractors. A major subcontractor is defined as one who will be providing critical hardware or whose subcontract is for more than 20% of the total proposed price. In either case, the prime contractor and proposed major subcontractors will be assessed individually and the results will then be assessed in their totality to derive the offeror's Past Performance rating.

(a) The Government will conduct a performance risk assessment based on the quality, relevancy and recency of the offeror's past performance, as well as that of its major subcontractors, as it relates to the probability of successful accomplishment of the required effort. Recent performance is defined as contracts performed and/or completed within the past three years. Areas of relevance include projects cited as comparable to the current program in terms of scope, complexity, and/or cost magnitude. When assessing performance risk, the Government will focus its inquiry on the past performance of the offeror and its proposed major subcontractors as it relates to all solicitation requirements. These requirements include all aspects of schedule, performance and supportability, including the offeror's record of: 1) conforming to specifications and standards of good workmanship; 2) maintaining program execution within cost and ability to forecast and contain costs; 3) adherence to contract schedules, including the administrative aspects of performance; 4) ability to resolve technical and manufacturing problems quickly and effectively; 5) business-like concern for the interest of its customers (i.e. commitment to customer satisfaction and cooperation between the offeror's organization and clients); and 6) establishing and maintaining adequate management of subcontractors.

(b) A significant achievement, problem or lack of relevant data in any element of the work can become an important consideration in the source selection process. A negative finding under any element may result in an overall high-risk rating. Therefore, offerors are reminded to include all relevant past efforts, including demonstrated corrective actions, in their proposal. Relevant performance is defined as contracts that are for efforts that have a logical connection with the efforts required by the solicitation.

(c) Offerors are cautioned that in conducting the performance risk assessment, the Government may use data provided in the offeror's proposal and data obtained from other sources. Since the Government may not necessarily interview all of the sources provided by the offerors, it is incumbent upon the offerors to explain the relevance of the data provided. Offerors are reminded that while the Government may elect to consider data obtained from other sources, the burden of proving low performance risk rests with the offerors.

(d) In the event an offeror has no record of relevant past performance or past performance is not available, the offeror will receive a neutral evaluation which will neither be favorable nor unfavorable.

M.4.4 Cost/Price Evaluation Approach. All proposed contract costs will be considered in the overall cost evaluation. The Government will analyze each offeror's cost and pricing information in terms of completeness, reasonableness, and realism. The Government will evaluate the realism of the offeror's proposed costs in relation to the offeror's specific technical approach. Any proposal, which is evaluated by the Government as significantly unrealistic in cost may be considered by the Government to reflect either a lack of technical competence to accomplish the Government's requirements or a failure to understand the Government's requirements, or both. The offeror's proposed cost will be evaluated by determining what the Government predicts the offeror's approach would most probably cost the Government when the work performed under the contract is completed. Offers that are determined to be materially unbalanced may be rejected. An offer is mathematically unbalanced if it is based on prices

which are significantly less than the cost for some contract line items and significantly overstated in relation to cost for others.

M.5 ORAL DISCUSSIONS.

M.5.1 General Information. Oral discussion sessions may be held, at the discretion of the Government, for each offeror determined to be in the competitive range. Since the oral discussion sessions constitute "discussions" in accordance with FAR 15.306(d) and 15.307(b), the Contracting Officer will request the submission of final proposal revisions. Final proposal revisions will be requested by the Government only after all oral discussion sessions are complete. Offerors will be allowed a minimum of two (2) calendar days to submit final proposal revisions.

M.5.2 Oral Discussion Scheduling. The Contracting Officer will schedule the oral discussion sessions to take place approximately 10 days after receipt of offers, and each offeror will be notified of the actual time and place at least three (3) days prior to their oral discussion session. Appropriate security clearances should be provided in sufficient time to process the requests. The contracting officer will provide additional instructions with the notification. The oral discussion sessions will be made at the Government's facility at TBD.

END OF SECTION M

ICIDS GLOSSARY OF ACRONYMS AND ABBREVIATIONS

Acronym	Definition
ACES	Access Control Equipment System
ACP	Access Control Point/Package/Program
ACS	Access Control System
AKA	Also Known As
AMC	Army Materiel Command
ANAD	Anniston Army Depot
AOR	Area of Responsibility
AP	Acquisition Plan
APG	Aberdeen Proving Ground
API	Applications Programming Interface Applications Programs Infrastructure
APM ( )	Assistant Product Manager ( )
AR	Army Regulation
ARCENT	Army Central Forces Command
ARP	Acquisition Requirements Package
AS	Acquisition Strategy
ASIS	American Society for Industrial Security
ASP	Ammunition Supply Point
ASR	Acquisition Strategy Report
ASSIST	Acquisition Source Selection Interactive Support Tool
AT/FP	Antiterrorism/Force Protection
ATO	Anti-Terrorism Officer
BCE	Baseline Cost Estimate
BGAD	Blue Grass Army Depot
BIT	Built-In Test
BITE	Built-in Test Equipment
BMS	Balanced Magnetic Switch
BMWS	Bistatic Microwave Sensor
BPA	Blanket Purchasing Agreement
BRAC	Base Realignment and Closure
CAC	Common Access Card
CAC-W	CECOM Acquisition Center-Washington
CBDCOM	Chemical, Biological Defense Command
CBMS	Chemical Biological Medical Systems
CCTV	Closed Circuit Television
CD	Compact Disc
CDP	Commercial Drawing Package
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CECOM	US Army Communications-Electronics Command
CENTCOM	Central Command

ICIDS GLOSSARY OF
ACRONYMS AND ABBREVIATIONS

CFE	Contractor Furnished Equipment
CIDS	Commercial Intrusion Detection System
CLA	Chemical Limited Area
CLIN	Contract Line Item Number
CM	Configuration Management/ Manager
CMA	Chemical Materials Agency
CMP	Configuration Management Plan
CMS	Configuration Management System
CONUS	Continental United States
COR	Contracting Officer's Representative
COTS	Commercial-off-the-shelf
CPD	Capabilities Production Document
CP-IPT	Cost/Performance – Integrated Product Team
CPU	Central Processing Unit
CSC	Computer Sciences Corporation
CWBS	Contract Work Breakdown Structure
DA	Department of the Army
DAS	Data Authentication System
DC	Direct Current
DCMA	Defense Contract Management Agency
DCO	Dial Central Office
DES	Data Encryption System
DFAS	Defense Finance Accounting Service
DIA	Defense Intelligence Agency
DID	Data Item Description
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DOIM	Directorate of Information Management
DOTM-E	Detection on-the-Move Exterior
DOTM-I	Detection on-the-Move Interior
DPG	Dugway Proving Ground (UT)
DPM	Deputy Provost Marshal
DPM	Deputy Program / Product Manager
DPW	Department of Public Works
DS	Door Strike
DSM	Display Screen Monitor
DTM	Data Transmission Media
DTRA	Defense Threat Reduction Agency
DVR	Digital Video Recorder
ECE	Entry Control Equipment

ECF	Entry Control Facility
ECP	Engineering Change Proposal
ECP	Entry Control Point
EMI	Electro-Magnetic Interference
EMMS	Exterior Microwave Motion Sensor
EOC	Emergency Operations Center
ESC	Electronic Support Center (USACE Army)
FAQT	First Article Qualification Test
FAR	False Alarm Rate
FAR	Federal Acquisition Regulation
FAT	First Article Test; Factory Acceptance Test
FFP	Firm Fixed Price
FLIR	Forward Looking Infrared
FM	Frequency Modulation / Field Manual
FMVS	Fence Mounted Vibration Sensor
FO	Fiber Optic
FOTE	Follow-on Test and Evaluation
FOV	Field of View
FPED	Force Protection Equipment Demonstration
FPO	Force Protection Officer
FPSS	Force Protection Sensor Selector
FRAB	Functional Requirements Authentication Board
FY	Fiscal Year
GAO	General / Government Accounting Office
GCE	Government Cost Estimate
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFM	Government Furnished Materiel
GSA	Government Services Administration
GWS	Grid Wire Sensor
HWAD	Hawthorne Army Depot, NV
HQ	Headquarters
HQ, AMC	Headquarters, Army Material Command
HQDA	Headquarters, Department of the Army
HQ, EUCOM	Headquarters, European Command
HQ, FORSCOM	Headquarters, Forces Command
HQ, USAEUR	Headquarters, US Army Europe
HVAC	Heating, Ventilation, and Air Conditioning
HVASC	High Value Asset Security Container
HWAD	Hawthorne Army Depot
IAW	In Accordance With

ICIDS GLOSSARY OF
ACRONYMS AND ABBREVIATIONS

IC	Integrated Circuit
ICC	Integrated Circuit Chip
ICD	Initial Capabilities Document
ICIDS	Integrated Commercial Intrusion Detection System
IDAS	Intrusion Detection/Assessment System
ID/IQ	Indefinite Delivery/Indefinite Quantity
IDE	Integrated Digital Environment
IDEWS	Intrusion Detection Early Warning System
IDS	Intrusion Detection System
IFN	Items for Negotiation
IGCE	Independent Government Cost Estimate
ILD	Internal Locking Device
ILS	Integrated Logistics Support
IMP	Integrated Master Plan
I/O	In/Out
IOC	Initial Operating Capability
IOT & E	Initial Operational Test & Evaluation
IPM	Intelligent Poller Multiplexer
IPR	In-Process Review
IPS	Integrated Program Summary
IPT	Integrated Product Team
IR	Infra-Red
ISP	Integrated Support Plan (in connection w/logistics)
ISR	Installation Status Report
IT	Information Technology
J-SIIDS	Joint Services Interior Intrusion Detection System
JPEO CBD	Joint Program Executive Office for Chemical and Biological Defense
JPMG	Joint Project Manager-Guardian
JRWG	Joint Requirements Working Group
JSIVA	Joint Services Integrated Vulnerability Assessment
KO	Contracting Officer
LAN	Local Area Network
LC	Local Controller
LCCE	Life Cycle Cost Estimate
LCCS	Life Cycle Cost Study or Life Cycle Contractor Support
LCD	Liquid Crystal Display
LE	Law Enforcement
LEAD	Letterkenny Army Depot
LED	Light Emitting Diode
LEMC	Letterkenny Munitions Center
LOS	Line-of-Sight
LPMC	Large Primary Monitor Console (ICIDS)

LPO	Lead Project Officer
MANSCEN	Maneuver Support Center (Fort Leonard Wood, MO)
MCAAP	McAlester Army Ammunition Plant
MCU	Master Communications Unit
MDEP	Management Decision Package
MDW	Military District of Washington
MEDCOM	US Army Medical Command
MEVA	Mission Essential Vulnerable Area Mission Essential Vulnerable Assessment
MFA	Materiel Fielding Agreement
MFP	Materiel Fielding Plan
MILCON	Military Construction
MIPR	Military Interdepartmental Purchase Requisition
MOA	Memorandum of Agreement
MOD	Modification
MOE&S	Measures of Effectiveness & Suitability
MOI	Memorandum of Instruction / Intent
MON	Memorandum of Notification
MOP	Measure of Performance
MOU	Memorandum of Understanding
MP	Military Police
MSR	Monthly Status Report
MTTR	Mean Time To Repair
MUX	Multiplexer
MWD	Military Working Dog
NAR	Nuisance Alarm Rate
NCO	Non-Commissioned Officer
NCOIC	Non-Commissioned Officer-in-Charge
NDA	Non-Disclosure Agreement
NDI	Non-Developmental Item
NEC	National Electrical Code
NEMA	National Electrical Manufacturers Association
NERD	Network Enabled Resource Device
NET	New Equipment Training
NETP	New Equipment Training Plan
NETT	New Equipment Training Team
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NLT	Not Later Than
NSN	National Stock Number
NVL	Night Vision Laboratory
OCONUS	Outside Continental United States
ODS	Online Data Storage

OIC	Officer In Charge
OMA	Other Maintenance, Army
ONS	Operational Needs Statement
OPA	Other Procurement, Army
OPMG	Office of Provost Marshal General
ORD	Operational Requirements Document
OSE	Other Support Equipment
OSHA	Occupational Safety & Health Agency
OTTR	Operational Test Readiness Review
OWS	Operator Work Station
PARC	Principal Assistant Responsible for Contracting
PAS	Product Assessment System or Personnel Alerting System
PAWS	Pager Alert Warning System
PBAS	Program Budget Accounting System
PC	Personal Computer / Printed Circuit
PCCS	Ported Coax Cable Sensor
PCD	Pueblo Chemical Depot
Pd	Probability of Detection
PEO, CS & CSS	Program Executive Office, Combat Support and Combat Support Services
PIC	Personal Identification Code
PIMS	Passive Infrared Motion Sensor
PIN	Personal Identification Number
PIR	Passive Infra-Red
PKI	Public Key Infrastructure
PM	Product/Program/Project Manager
PM	Provost Marshal
PM	Processor Motherboard
PMC	Primary Monitoring Console/Cabinet
PMCS	Preventive Maintenance Checks and Services
PMO	Provost Marshal Office
PM-FPS	Product Manager, Force Protection Systems
POC	Point of Contact
POM	Program Objective Memorandum
POP	Period of Performance
PSE	Physical Security Equipment
PSEAG	Physical Security Equipment Action Group
PSR	Program Status Review
PSS	Physical Security System/Pre-Site Survey
PSV	Perimeter Security Veil
PTZ	Pan-Tilt-Zoom
PVT	Performance Verification Test
QA	Quality Assurance
QC	Quality Control

QRM	Quarterly Review Meeting
RADC	Remote Area Data Collectors
RAM	Random Access Memory
REX	Request to Exit Device
RF	Radio Frequency
RFP	Request for Proposal
RIA	Rock Island Arsenal
RIAD	Rock Island Army Depot
RIOX	RADC Input/Output Expansion Module
ROM	Read Only Memory
ROM	Rough Order of Magnitude
RRAD	Red River Army Depot
RSM	Remote Status Monitor
RTE	Request to Exit
SA	System Administrator
SAP	Special Access Program
SAPF	Special Access Program Facility
SAR	Safety Assessment Report
SAR	Significant Activity Report
SAT	System Acceptance Test
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SEIWG	Security Equipment Integration Working Group
SFR	System Functional Review
SMDC	Space & Missile Defense Command
SME	Subject Matter Expert
SOP	Standing Operating Procedure
SOW	Statement of Work
SPMC	Small Primary Monitor Console
SPV & E	System Performance Verification & Endurance
SPAWAR	US Naval Space and Warfare Command
SPS	System Performance Specification
SSA	Source Selection Authority
SSAC	Source Selection Advisory Committee
SSCC	Site Security Control Center
SSD	Site Specific Design
SSEB	Source Selection Evaluation Board
SSV	Site Survey Verification
SUPR	Supervisor Station
SVR	System Verification Review
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol

TDY	Temporary Duty
TEMP	Test and Evaluation Master Plan
TM	Technical Manual
TOQ	Top of Queue
TRADOC	US Army Training and Doctrine Command
TRR	Test Readiness Review
TS	Top Secret
TSE	Tactical Security Equipment
TSWG	Technical Support Working Group
UGS	Unattended Ground Sensor
UI	User Interface
UII	Unique Item Identification
UL	Underwriters Laboratory
UMCD	Umatilla Chemical Depot
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
USACE	US Army Corps of Engineers
USAREUR	US Army, Europe, and Seventh Army
USAMPS	US Army Military Police School
USMA	US Military Academy, West Point
V-LAN	Virtual Local Area Network
VCR	Video Cassette Recorder
VIP	Very Important Person
VTC	Video Tele-Conference
WBS	Work Breakdown Structure
WPR	Weekly Progress Report
WRAMC	Walter Reed Army Medical Center
WSMR	White Sands Missile Range

DRAFT

31 OCTOBER 2005
Rev. 0
ICIDS-PS-0600

PERFORMANCE SPECIFICATION

FOR

COMMAND, CONTROL, AND DISPLAY SUBSYSTEM

OF THE

INTEGRATED COMMERCIAL INTRUSION

DETECTION SYSTEM IV

DRAFT v7

Solicitation Number

TABLE OF CONTENTS

1. SCOPE.

This Performance Specification (PS) specifies the major component requirements for the Command, Control, and Display Subsystem (CCDS) of the Integrated Commercial Intrusion Detection System (ICIDS). It establishes the performance, interface requirements and test requirements for the ICIDS CCDS. The ICIDS major components are:

a. Primary Monitor Console (PMC)
b. Console Uninterruptible Power Supply (UPS),
c. Remote Area Data Collector (RADC), and
d. Remote Status Monitor (RSM) with UPS.

External interface requirements to sensors, sensor stimuli, response devices, deterrent devices, Closed-Circuit Television (CCTV), Entry Control Equipment (ECE), Radio Frequency/Microwave and Fiber Optic Communication networks are specified herein. Performance requirements for the sensors, CCTV, and ECE are described in separate documents.

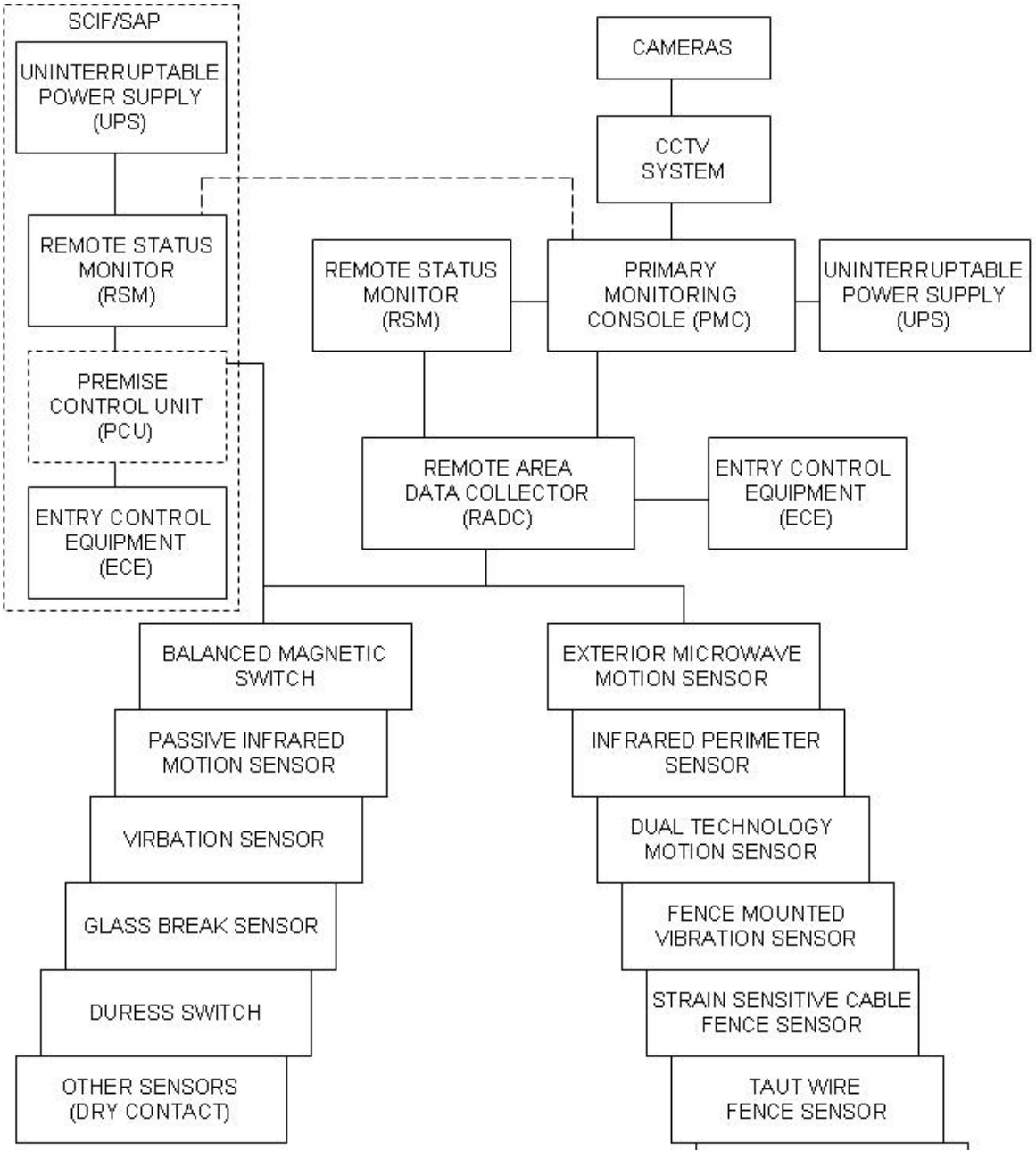
The CCDS configuration depends on the site size and the required security level. Figures 1 and 2 depict typical ICIDS components used in an ICIDS configuration.

2. APPLICABLE DOCUMENTS.

2.1 Government Documents.

2.1.1 Specifications, Standards, and Handbooks.

The following documents, of the issue in effect on the date of the request for proposal, form a part of this PS to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the Department of Defense Index of Specifications and Standards (DODISS) and supplement thereto.



NOTES:
1. DIAGRAM DESCRIBES FUNCTIONAL REQUIREMENTS AND IS NOT A DESIGN CONSTRAINT.
2. QUANTITIES AND TYPES OF COMPONENTS WILL VARY WITH EACH INSTALLATION.
3. TRANSMISSION MEDIA IS NOT SUPPLIED UNDER THIS CONTRACT.
4. PCU (USED ONLY IN SCIF/SAP) SERVES SAME FUNCTION AS RADC

ICIDS COMPONENTS

SPECIFICATIONS

FEDERAL

FCC Part 15	08 December 2003	Federal Communications Commission (FCC) Rules and Regulations.

Department of Defense (DoD)

DoD C 5210.41-M	31 March 1983	Nuclear Weapon Security Manual

US ARMY

DA form 4930-R:	30 September 1980	Alarm/Intrusion Detection Record
AR 190-11	12 February 1998	Physical Security of Arms, Ammunition, and Explosives
AR 190-13	30 September 1993	The Army Physical Security Program
AR 380-381	21 April 2004	Special Access Programs (SAPS) and Sensitive Activities.
AR 190-59	01 JULY 1998	Chemical Agent Security Program
ICIDS-PS-0601	31 October 2005	Performance Specification for Closed Circuit Television Assessment Equipment of the Integrated Commercial Intrusion Detection System.
ICIDS-PS-0602	31 October 2005	Performance Specification for Entry Control Equipment of the Integrated Commercial Intrusion Detection System.

Numbered PES	January 2002 Rev. 2	Performance Equivalence Sheets for ICIDS-IV provide minimum performance characteristics for interior and exterior sensors.
DAMI-CDS Memorandum	01 March 2004	Updated Guidance for Installation of ICIDS in Army Sensitive Compartmented Information Facilities (SCIFs).

STANDARDS

FEDERAL

Federal information processing standard publications:

FIPS PUB 46-3	25 October 1999	Data Encryption Standard.
FIPS PUB 140-1	11 January 1994	Security Requirements for Cryptographic Modules.

These documents can be found at the following web address: http://csrc.nist.gov/publications/fips/index.html

2.1.2 Other Government Documents, Drawings and Publications.

The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise indicated, the issues are those in effect on the date of the solicitation.

Director of Central Intelligence Directives (DCID):

DCID 6/9	18 November 2002	Physical Security Standards for Sensitive Compartmented Information

Facilities (SCIF).

(Copies are available at the Program Office [PM-FPS] for review).

Joint Air Force, Army, and Navy Documents:

JAFAN 6/9	23 March 2004	Joint Air Force-Army-Navy Physical Security Standards for Special Access Program Facilities

Army Corps of Engineers Guide Specification:

UFGS-16768A	April 2004	Fiber Optics Data Transmission Media for Security Systems, Including Changes of Notice

(Guide Specifications may be accessed through the U.S. Army Corps of Engineers web site at: http://www.ccb.org/docs/ufgshome/UFGSToc.htm)

Training and Doctrine Command Documents:

ICIDS Operational Requirements Document (ORD) 04 October 1994

Integrated Commercial Intrusion Detection System (ICIDS):

ICIDS	22 July 2005	ICIDS Security Classification Guide

2.2 Non-Government Publications.

The following documents form a part of this PS to the extent specified herein. Unless otherwise specified, the issues in effect on the date of the invitation for bids or request for proposal shall apply.

Underwriters Laboratories (UL) Standards:

UL 634	23 February 2000	Connectors and Switches

		for Use with Burglar-Alarm Systems, 8th Ed.
UL 639	21 February 1997	Intrusion-Detection Units, 7th Ed.
UL 1076	29 September 1995	Proprietary Burglar Alarm Units and Systems.

(Application for copies should be addressed to Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062.)

National Electrical Code (NEC) 2005

National Electrical Manufacturers Association (NEMA):

NEMA 250-2003	Enclosure for Electrical Equipment (1000 v max).

(Application for copies should be addressed to National Electrical Manufacturers Association, 2101 L Street NW, Suite 300, Washington DC 20037.)

National Fire Protection Association (NFPA)

NFPA-70 2005	National Electrical Code.

(Applications for copies should be addressed to the National Fire Protection Association, International, 60 Batterymarch Street, Boston, MA 02110.)

(Non-government standards and other publications are normally available from the organizations which prepare or which distribute the documents. These documents may also be available in or through libraries or other informational services.)

2.3 Order of Precedence.

In the event of a conflict between the text of this PS and the references cited herein, the text of this PS shall take precedence. Nothing in this specification, however, shall supersede applicable laws and regulations unless a specific exemption has been obtained.

3. REQUIREMENTS.

3.1 Description.

The system consists of equipment in the monitor functional area, communications functional area, and remote functional area. The CCDS configuration described herein is intended to illustrate functional requirements only and is not intended as a design constraint. All system components fall into one or more of these functional areas.

a. The monitor functional area equipment, through sequential polling, receives, processes, and displays remote area and system data. It executes command and control functions either automatically or under operator control. The monitor functional area equipment shall employ Open System Architecture.

b. The communications functional area equipment spans the distance from the monitor area to the remote areas.

c. The remote functional area equipment generates alarm and status change signals in response to local phenomena and collects and transmits this data. Selected remote area equipment also receives operator-commanded actions and executes operator-commanded actions.

The CCDS components shall each provide methods of self-protection, either individual or distributed. This protection shall include methods of component tamper security and inter-component communication link tamper security. System component design shall incorporate means of protecting the integrity of all communication links (e.g., line supervision, encryption).

All communication, power, and other interface lines shall be provided with Electromagnetic Interference (EMI), transient, and surge protection, in accordance with paragraph 3.11, to prevent damage to equipment from lightning and other conducted electrical disturbances, or to localize damage in easily repairable low-cost components.

3.1.1 Major Component Groups.

The system contains:

a. Primary Monitor Console (PMC) capable of communicating over Government supplied communications media, including metallic wire pairs. Salient characteristics typical of metallic pairs are summarized at Attachment 1.

b. Remote Area Data Collectors (RADCs) capable of communicating over Government supplied communications media, including metallic wire pairs. Salient characteristics typical of metallic pairs are summarized at Attachment 1.

3.1.2 Other Components.

The CCDS may include any or all components specified herein, and shall interface and perform with the following components, as required, to form a complete ICIDS:

a. Remote Status Monitors (RSM) (see paragraph 3.4.2.3)

b. Sensors (see PES Nos. 1-14 and 21-30)

c. Data Authentication System (DAS) (see paragraph 3.5 herein)

d. Automated Entry Control Equipment (ECE) (see ICIDS-PS-0602)

e. Closed Circuit Television (CCTV) system (ICIDS-PS-0601)

f. Radio Frequency (RF)/Microwave Communication Link (see paragraph 3.6 herein)

g. Fiber optic communication interface (fiber optic cable is provided by the installation site) (see paragraph 3.7 herein)

h. Uninterruptible Power Supply (UPS) (see paragraph 3.4.2.1.10)

3.1.3 System Configurations.

The CCDS shall provide for expansion and flexibility of application to adapt to individual site characteristics. The interface and functional requirements, specified herein, apply to all CCDS, except as explicitly noted herein.

For the purposes of this PS, the two site characteristics which impact CCDS functionality and configuration are site size and security level. The system diagram, shown in Figure 2, depicts the configurations that conform to the requirements for each of the four security levels and accommodates several user options (e.g., DAS, ECE, RADCs, and CCTV).

The four levels of security depend upon the assets being secured. The system configuration of Figure 2 and the applicable military requirements collectively define the equipment necessary to secure sites of all four security levels IAW AR 190-13, Chapter 4.

3.2 Construction.

The CCDS Construction shall meet the conditions specified in UL 1076, Sections 5 through 9.

3.3 Reliability and Maintainability.

3.3.1 Logistics and Readiness Requirements.

The ICIDS shall have a system operational availability (Ao) of 0.997 or greater, a mean time to repair (MTTR) of 0.5 hours, a maximum time to repair (MAX TTR) of 1.0 hours, a direct support maintenance ratio (MR) of 0.16 for the PMC and a service life of not less than 10 years. The initial mean time between operational mission failure (MTBOMF) for the display subsystem shall be 4,100 hours, a mean time between failure (MTBF) for any single transmission line of 21,400 hours, an MTBF for the RADC of 11,100 hours, and an MTBF for any sensor of 18,100 hours. Logistics and maintenance support will be accomplished by turn key contract or local contractual agreements at the installation level. The ICIDS integrated logistics support (ILS) plan will be tested during the initial operational test and evaluation of the system.

3.3.2 Failure Definition.

Failure is defined as any malfunction that results in loss of the ability of the equipment to perform its intended function.

3.3.3 Maintainability Characteristics.

The CCDS components shall incorporate features that enable cost effective maintenance throughout their deployed life. CCDS component maintainability features include:

a. Equipment shall remain operational during maintenance with all maintenance access covers, plates, doors, etc., removed or opened.

b. All indicators, which operator and maintenance personnel normally replace, shall be readily accessible.

c. Protective covers shall be installed over external connectors on remote area equipment with all-weather enclosures to prevent inadvertent damage or contamination.

d. Sized and keyed electrical connectors, plug-in assemblies, and controlled cable length shall be used to preclude mating to wrong receptacles.

e. Cable connectors and receptacles shall be marked with unique numerical designations to facilitate inspection and assembly. Labels and warnings shall be visible when the component is assembled.

3.3.4 Preventive Maintenance.

System components shall require minimal preventive maintenance. Provisions to perform preventive maintenance, while the system is operational, shall be provided.

3.3.5 System Endurance.

The system shall be capable of continuous operation (24 hours per day, 365 days per year) for the life expectancy of ten (10) years (minimum) with proper corrective and preventive maintenance.

3.3.6 Fault Detection/Fault Isolation (FD/FI).

FD/FI shall be incorporated to determine faults to the Line Replaceable Unit (LRU) (see 6.4.1).

3.4 Command, Control, and Display Subsystem (CCDS) Performance Characteristics.

3.4.1 General System Requirements.

3.4.1.1 To Report.

The CCDS installed in any ICIDS site, operated and maintained in accordance with established procedures, shall report detection of intruders, tampering, and equipment malfunctions. All detection information shall be processed and displayed to the operator of the system.

3.4.1.2 To Assess.

The system shall permit the operator to assess the nature of the intrusion via assessment devices, such as CCTV. The system design shall allow for automatic and manual control of assessment devices at the user's option. The operator shall not be able to manually activate the video assessment devices unless the remote area is in the Secure mode of operation or an alarm is present. Allow a duress alarm to be output by the entering of a special code into a key pad or by activating a panic switch. Display the duress alarm at the network controller and operator console, but provide no indication of duress alarm at the local controller or key pad.

3.4.1.3 To Deter.

The system shall provide four interfaces to control various response devices that deter or delay accomplishment of intrusion into protected area. The system design shall allow for manual operation of the response devices. The operator shall not be able to manually activate the response devices unless the remote area is in the Secure mode of operation and an alarm is present.

3.4.1.4 System Timing.

The requirement for the system timing, via the RADC to PMC path, shall be any single alarm up to any five simultaneous alarms transmitted, processed and annunciated within a maximum total of 3.0 seconds after the alarms occurs.

a. If the RSM receives system status through the PMC, then the system timing via the PMC to RSM path shall be such that any single alarm is transmitted, processed and annunciated at the RSM within a maximum total of 2.0 seconds after display at the PMC. If the RSM communicates directly with the RADCs, then the system timing via the RADC to RSM path shall be such that any single alarm is transmitted, processed and annunciated within a maximum total of 3.0 seconds after the alarm occurs at the RADC. Neither RSM timing requirement shall increase the maximum PMC annunciation time.

b. The PMC shall interface to the CCTV switcher in a manner that requires the display of associated video within 1.0 second after the alarm is displayed.

3.4.1.5 Tamper Protection.

All CCDS components specified herein shall have tamper protection, unless otherwise specified. All removable panels, doors, drawers, or other access openings shall be equipped with tamper switches. The tamper switches on panels and doors shall be installed and baffled to prevent access, for defeating the switch, by deforming or opening the door or cover. The tamper switches shall be corrosion resistant to the environment to which they will be exposed. Tamper switches shall have maintenance positions that allow performance of maintenance tasks with the system fully operational. All doors shall be equipped with double action, high security locks. Information regarding approved locks shall be obtained from the Naval Facilities Engineering Service Center (NFESC), ATTN: Code ESC66, 1100 23rd Avenue, Port Hueneme, CA 93043-4370. The use of any master key system or multiple key system is prohibited.

3.4.1.6 Printer.

Multiple printers are permitted. The printer shall provide the following capabilities:

a. Event printing: The printer shall be capable of printing record all significant system activity (alarms, status changes, etc.) including date,

time and all operator actions, whether displayed or not.

b. Log printing: The printer shall also have the capability to allow the operator, maintainer or supervisor, under key, password or other control, to print reports of historical system data selected from a number of pre-defined (ex. DA form 4930-R: Alarm/Intrusion Detection Report) or user-defined formats and contents.

3.4.2 CCDS Major Components.

3.4.2.1 Primary Monitor Console (PMC).

3.4.2.1.1 Description.

The PMC is a monitor area item and shall utilize an interrogate-response polling sequence to provide the primary command and control for the secure areas, hereafter called remote areas. The PMC shall have the capability to monitor up to at least 512 remote areas controlled by RADCs.

3.4.2.1.2 Functional Areas.

The major functional areas of the PMC are:

a. Command, Control, and Display (CCD),

b. operator interface including operator input devices, maintenance input devices, video status display, geographic and remote area graphic display, CCTV controls and monitors, and audible alarms and printer,

c. remote area communication,

d. interconsole communication (PMC to RSM[s]), and

e. system data storage.

3.4.2.1.3 Command, Control and Display Functions.

The Command, Control and Display functions shall be to:

a. Supervise all PMC, RADC, and RSM communications and data flow.

b. Communicate with the remote areas (RADCs) by way of pseudo-random generated tones or digital encoding using an interrogate and response protocol to determine the status of each remote area, and annunciate all status changes. Status changes include, but are not limited to, alarm, ACCESS/SECURE/OFF-LINE, and entry denied.

c. Provide the communication interfaces to connected RADCs and RSMs with the following capabilities:

(1) Send and receive data by one of the following separate data link interfaces and subsystems. The PMC is required to support any combination of the following data links, as selected by the user. The choice of data link shall be made by the user and shall not limit any system performance nor preclude the use of the DAS, whether internal or external:

(a) Interfaces with continuous metallic wire pairs are required for all data links of the PMC. Salient characteristics typical of metallic pairs are summarized at Attachment 1.

(b) A commercial RF/microwave data link may be specified, prior to installation, for some or all remote area or PMC-to-RSM communication links. It shall be compatible with the metallic wire pair interfaces at the PMC, RSM, and RADC.

(c) A commercial fiber optic communication interface is an option to be specified by the user for some or all remote area or PMC-to-RSM data communication links. The transmit/receive circuitry which interfaces to the fiber cable may be internal (e.g., replaces hardwired modem) or external (e.g., connects to PMC hardwired output). It shall be compatible with the PMC, RSM and RADC data communication interfaces. The fiber optic communication interface shall utilize

fiber optic cable and components as specified in CEGS-16768, Fiber Optic Data Transmission System for Security Systems.

(2) Execute error detection and line supervision processes in order to monitor, detect, and report the loss of line integrity of the communication links.

(3) The PMC-to-RADC and PMC-to-RSM links (as architecture dictates) shall be capable of operating up to 16 kilometers without repeaters or relays.

(4) Exchange information over the RADC interface including:

(a) Sensor alarms

(b) Sensor tamper

(c) RADC status including ACCESS/SECURE/OFF-LINE mode

(d) RADC tamper

(e) RADC power supply fail alarms

(f) Response device commands

(g) Response device status

(h) Remote area configuration

(i) Self-test commands and results

(j) Entry Control Equipment data (e.g., entry approved/denied). The PMC shall be notified of any shunted RADC or sensor.

(5) Exchange information over the RSM interface including all, or user-selected, portions of the system status. The user selects the information to be passed over this link at the time of initial system configuration, and it is a maintenance function to configure the PMC and/or RSM to implement these selections.

(6) Provide an interface for the optional use of the DAS with any or all of the communication links.

For ICIDS installations with SCIF remote areas, which are not located in areas within Government controlled facilities within CONUS, the DAS Type I line supervision is required for all RADC communication links which are routed outside the SCIF (see DCID 6/9).

For ICIDS installations with the PMC and RSM installed within a SCIF, Type II B line supervision is required for all PMC-to-RADC data links (see DCID 6/9).

d. Monitor the tamper conditions for the PMC and PMC power supply.

e. Monitor AC power status for the PMC.

f. Monitor operator input device data, such as commands and requests.

g. Provide the capability to assign a priority level to each RADC. The PMC shall display alarms, according to this priority, regardless of the sequence of arrival. A minimum of four levels of priority are required. Alarms of the same priority shall be displayed in the sequence of arrival.

h. Support the RADC interface to Entry Control Equipment (ECE). The PMC shall receive and display entry control information including, but not limited to, entry approved, entry denied alarms, and tamper from the RADC. Functions required of the ECE may be implemented at either the PMC or RADC, but, in all cases, ECE data and processing shall be subordinated in priority to intrusion data and processing. The processing of ECE data at the PMC shall not affect the system timing requirements. Functional requirements for the ECE system are specified in ICIDS-PS-0602.

i. Provide an interface with a CCTV system that shall perform as described in 3.4.2.1.11. Functional requirements for the CCTV system are specified in ICIDS-PS-0601.

j. Automatically activate the video cameras, upon receipt of the first alarm from the remote areas, to enable operator assessment of remote area alarms from remote areas equipped with cameras. In the case of multiple alarms, means shall be provided to allow the operator to manually select the video for each subsequent alarm. New alarms, regardless of priority, shall not take precedence over alarms currently being addressed by the operator nor automatically change the status or geographic displays; the video for the new alarm(s) shall be activated only upon manual operator selection.

k. Provide an interface for a printer(s). The PMC shall print a hard copy of all system activity, including operator actions. The PMC shall also have the capability to allow the maintainer or supervisor, under key, password, or other control, to print reports of historical system data. When the printer is OFF-LINE or printing requested reports, data shall continue to be stored for retrieval when the printer is restored ON-LINE.

l. Print or display the system configuration data, including date and time, of the most recent system configuration changes.

m. Provide for orderly shutdown and restart whenever components are replaced or have lost information because of power failure or component failure.

n. Provide for automatic, nonvolatile data storage of historical data, system configuration data, and system status such as graphic maps, CCTV maps, configuration tables, databases, periods of maintenance, and sensor shunting. The operator shall have no control of data storage. Access to replacing, printing, or backing up the historical data shall be restricted to personnel with the appropriate level of access.

o. Have provisions for automatic storage of system configuration data and automatic reinitialization of system configuration from data storage after any system outage (i.e., power outage or system maintenance downtime). Reinitialization time from

power on until full system operation shall not exceed five minutes.

p. Provide for both a manual and an automatic self-testing of the system with the capability for user definable and programmable parameters at installation. These parameters shall include duration of test, number of tests per a given time period, and other required system test parameters data. The interval between automatic tests shall be randomized. Annunciation of intentional alarms generated on a specific device, while under self-test, shall be suppressed. Any valid alarm such as intrusion, tamper or duress (other than an intentional alarm), generated during a self-test, shall cause the self-test to terminate and the alarm shall be annunciated. The results of all self-tests shall be recorded on the printer and in the system data storage. Only self-test failures shall be annunciated at the PMC status displays. Any mode change from ACCESS to SECURE shall automatically initiate a self-test of the remote area equipment within 90 seconds after the mode change.

q. Provide for two processes to change the ACCESS/SECURE mode of operation of a RADC for an individual sensor or for the entire RADC: 1) from the PMC or RSM in CCD mode, or 2) from the RADC. The functional requirements of the ACCESS and SECURE modes are described herein and shall be implemented at the RADC regardless of the process used to change the mode.

The operator shall have the capability to change the ACCESS/SECURE mode of a remote area or sensor by entering a command at the PMC (except for SCIF areas where remote commanded ACCESS/SECURE is prohibited or locked-out at installation). The two-person rule requirements shall apply to commanded ACCESS/SECURE mode changes when so configured at installation.

Both of these operating mode changes shall be handled identically. The PMC shall monitor and continuously display the mode of operation of the sensors and RADCs. SECURE mode shall be indicated by green color for icons, indicators and graphics; ACCESS shall be indicated by yellow color,

r. Provide EMI, transient, and surge protection on all external interface lines, in accordance with paragraph 3.11.

3.4.2.1.4 Operator Interface.

The PMC command and control devices shall provide an integrated operator interface and provide at least four levels of access to operator functions. Access to each level shall be regulated by passwords or other means such that an operator possessing the lowest level of access may perform the minimum functions necessary to operate the system, and the other functions may be individually allocated to any of the other access levels. The system shall be able to support at least 25 passwords, each assigned to an access level. An operator with a password assigned to one access level can use the functions allocated to that and all lower levels, but shall not be able to use the functions allocated to any higher level. The system shall prepare a report presenting the available data required on DA Form 4930-R, Alarm Intrusion Detection Record. The report shall be populated by the available system data for each alarm reported via the alarm queue. This report shall provide space for the operator to add additional data that is not provided by the ICIDS system.

a. An operator input device (mouse, keyboard, or other) to implement the command, control, and display functions is required to issue commands. All operator functions shall be selected via dedicated or extensible function keys, mouse click, or other means. No operator actions shall require memorization of command strings and shall be tied to a minimum number of key-strokes (e.g., 1 or 2.). In addition, only one action (key stroke or mouse click) shall be required to acknowledge an alarm. The operator controls shall be clearly labeled as to their function. General purpose keyboards or specialized keyboards are permitted. The operator, with proper password, shall have the capability to selectively address the remote areas for such purposes as:

(1) Placing remote areas or specific individual sensors in ACCESS or SECURE mode (except as prohibited for SCIFs in paragraph 3.4.2.2.8). The user, at initial system

configuration, assigns to each RADC either unrestricted or two-person rule requirements for the ACCESS\SECURE mode changes. The unrestricted assignment allows a single PMC operator to command mode changes without the need for concurrence.

The two-person rule assignment shall implement the DoD and service requirements specified herein. This capability shall be provided as a user option, selectable for specific remote areas or specific individual sensors at initial system configuration. When this option is selected, a single PMC or RSM operator shall be prohibited from commanding remote areas or individual sensors OFF-LINE (e.g., for maintenance) or into ACCESS.

Two-person commanded ACCESS and commanded OFF-LINE from the PMC shall require cooperative action between two persons, either both at the PMC, or one person at the PMC and one person at the RSM, or both persons at the RSM (when in the CCD mode). When an operator commands (requests) a remote area or sensor into ACCESS or OFF-LINE, the second person (another operator, supervisor, or other authorized party) shall have means to concur with the command (acknowledge the request) within a reaction time period of 2 to 12 seconds (adjustable at initial system configuration) for the commanded action to take effect or be successfully completed.

In the absence of concurrence by the second operator before the reaction time, both audible and visual alarms at both consoles indicating a two-person rule violation shall be annunciated. The commanded action shall then be locked out and the violation alarms remain active until the operator, initially requesting the action, removes the request. Removal of the request shall automatically clear the alarm.

In the two-person rule process, the initial action is considered a request for the status or mode change. For the PMC or RSM initiating the action, the request is identical to the command or action used when two-person rule is not required. The concur action can take the form of a password entry, key switch or other dedicated process by a person other than the operator at the requesting PMC or RSM; or by a command key, password entry, or other action at the RSM. In all cases, the two-person rule design and implementation shall ensure the integrity and security of the intended process.

(2) Initiating a remote area sensor test and selectively initiating tests of system functions. This shall be in addition to periodic automatic testing.

(3) Activating response devices. The PMC shall provide the operator control to enable and disable, and activate or deactivate remotely controlled response devices. A response device must first be manually enabled by a PMC command before it can be manually activated. The PMC operator shall have the capability to activate a response device after correctly entering the activate command for the specific response device desired only when the RADC is in SECURE mode, the response device has been previously enabled, and an alarm is present.

(4) Acknowledging and resetting status changes. The operator shall be provided the capability to selectively acknowledge and reset alarms and status changes in order to return the system functions to their normal operating state. Acknowledging is defined as a PMC operator action using a single action to silence the audible alarm, and changes the displayed status of the event (alarm, AC power, etc.) from active (flashing red) to pending (steady red). A pending alarm is defined as an alarm that has been acknowledged (audio alarm

silenced), but not reset. The graphic and status messages for a pending sensor alarm shall change to flashing red when the sensor re-alarms. All alarms and status changes shall be acknowledged before they can be reset. Resetting an alarm is defined as a PMC operator action (e.g., a keystroke), which changes the displayed status of the event from pending (steady red) to clear or reset (steady green) and returns the sensor or device to the ready state. The PMC shall not allow any active alarm to be reset. The acknowledge and reset functions shall be provided for operator selected groups of RADCs.

(5) Selectively display individual remote area status or the primary screen on the status display, and provide the capability for the operator to access additional display screens as required. The primary screen is that which is normally shown on the status display; it contains the alarm display and system summary information detailed in paragraph 3.4.2.1.7. Individual remote area status screens and additional (secondary) display screens, shall contain such information as operator instructions, response force information, and details of the alarm zone. In the event of a new alarm, the display shall not automatically revert from secondary screens to the primary screen.

b. A maintenance input device (mouse, keyboard, or other) to permit a maintenance technician to perform required maintenance tasks. Unauthorized access to the maintenance input device shall be protected against by a mechanical and/or electrical lock (e.g., password, locked panel, etc.).

The PMC shall provide access to maintenance functions. Access shall be regulated by password or other means.

The PMC shall be capable of allowing all maintenance tasks except initial configuration to be accomplished while the PMC is on-line and fully operational. On-line maintenance shall not interfere with normal system operation nor cause the loss of any real-time or historical system data. The maintenance tasks shall include:

(1) Setting the time and date.

(2) Establishing, backing up, modifying, reloading (restoring) and recording (saving) the system configuration (database). All activities and parameters identified within this PS, which are established at initial system or device configuration, may also be modified by maintainers with the proper access level while the PMC is on-line.

(3) Graphic display generation.

(4) System initialization and reinitialization.

(5) Setting self-test parameters.

(6) System self-diagnostics (shall be disabled for RADCs installed in SCIFs).

(7) Printing various reports of historical system activity from system data storage.

(8) Selecting the portion of the PMC display to be displayed at RSM (if accomplished at PMC).

c. A video status display, a primary source of system information for the operator. The performance requirements of the status display are specified herein.

d. The video geographic map display for use by the operator to assess alarm location within the remote area and geographically within the site to assist in dispatching response teams. This single display shall be used for both the remote area graphic display and the geographic map display.

e. CCTV controls and monitors for operator assessment for remote area alarms that allow automatic alarm-triggered and manual operator-triggered selection of any camera onto any of four monitors. A fifth monitor shall be used for viewing video storage system images.

f. Audible alarm (audible tone signals) for annunciation of all alarms and system status changes. A dedicated control shall be provided to adjust the auditory signal volume to be easily heard above any expected ambient noise. A control shall be provided (e.g., acknowledge key) that silences the audible alarm for the current event only (alarm, status change, etc.). The audible alarm shall be activated for each new alarm. For repeated alarms, the audible alarm shall be reactivated to indicate any change in state of any alarm (e.g., from pending (acknowledged) to active (alarmed)).

g. A printer is required to provide a permanent record of all operator and system activity at the PMC, and as a secondary display for the operator in the event of a primary display failure. Multiple printers are not prohibited. The printer shall provide controls for the operator to put the printer ON-LINE/OFF-LINE for adding paper and clearing paper jams. When the printer is OFF-LINE, or printing requested reports, system activity shall continue being stored for later retrieval.

3.4.2.1.5 Remote Area Communication.

The PMC shall:

a. interface with system RADCs,

b. interface with collocated ECE, and

c. interface with a DAS to encrypt/decrypt all PMC-to-RADC data communication over that DAS data link. The DAS may be used on any or all PMC-to-RADC data links. Disruption or loss of this communication link shall be annunciated at the

PMC and RSMs as a line security alarm. When communication is lost or tampered between RADCs and remote area devices (e.g., sensors), a tamper or other distinct alarm shall be displayed at the PMC and RSMs.

3.4.2.1.6 Interconsole Communication.

The PMC shall:

a. Communicate (directly, if architecture dictates) all or selected portions of the system status, and all PMC operator actions for use by the RSMs.

b. Interface with a DAS to encrypt system data for use by the RSMs. Disruption or loss of these communication lines shall be annunciated at the PMC and RSMs as line security alarms.

c. Provide system status data for use of up to 8 RSMs on links capable of operating up to 16 kilometers without repeaters or relays.

d. The PMC shall provide the capability, upon configuration at the user's option, to automatically assume control of all remote areas upon failure of the RSM in CCD mode; or, to automatically relinquish control to an RSM(s) in CCD mode upon failure of the PMC. Control shall be capable of being switched to and from the RSM, either manually or automatically (according to a schedule or due to failure of PMC or RSM); however, the switchover shall not disrupt the continuous monitoring of RADCs or cause loss of any system data.

3.4.2.1.7 Status Display.

The PMC shall provide a dedicated visual status display, in color, which provides all of the remote area and system status information. The display format shall provide for rapid operator comprehension. This shall include the use of color, blinking fields, highlights, and other techniques to draw attention to alarms and status changes. The PMC status display shall:

a. Continuously provide the operator with summary status information for the complete system including alarm data on a time, location and component basis. Components for which alarms must be reported in the system summary include sensors, sensor loops, RADCs, UPSs, communication lines, and any system component that reports or is monitored for alarm. Alarm types include intrusion, tamper, line security, communication fault/failure, input power status (AC/DC), and other alarm types. Other status messages include ACCESS/SECURE/OFF-LINE mode for RADCs and sensors, maintenance mode for RADCs, power source (AC/DC) for PMC and RADCs, shunted sensor(s), and other potential status messages.

b. Display alarms in prioritized order independent of the sequence of arrival at the PMC. Alarms of the same priority shall be displayed chronologically within that priority level (see also 3.4.2.1.3.g). Alarms shall remain displayed until reset. Automatic prioritization of alarms in at least four user-defined levels is required (i.e., any subsequent alarms must be automatically organized on the status display in the prioritized order without requiring operator action).

c. Display, upon command, the status of each individual sensor and response device.

d. Display each status change as it occurs.

e. Display any special instructions for actions to be taken. This message shall be input by the PMC maintainer during system configuration.

f. Provide response device status (e.g., armed, disarmed, fired, safe).

g. Echo all operator inputs.

h. Display entry denied alarms and other ECE data at a priority level subordinate to intrusion alarms.

i. Continuously display an indication for the duration each RADC is in maintenance mode.

Continuously display all RADCs and sensors that have been shunted.

j. Contain text consisting of standard typewriter alphanumeric characters in upper and lower case. The text font and size shall produce an 80 column by 25 line display, and each character shall be displayed in any of 16 colors, selected by the user, except where previously defined in this performance specification.

k. Utilize a color visual display of at least 48 centimeters diagonal in size with a minimum resolution of 1280 X 1025 pixels.

3.4.2.1.8 Geographic Map Display.

The PMC shall provide a geographic map display that depicts each remote area by a representative map of the remote area, including surroundings. The geographic map display shall:

a. Provide a unique remote area graphic for each remote area to be created and edited by the user. Each graphic shall consist of text, symbols, lines and areas selected and placed by the user. The text shall consist of standard typewriter alphanumeric characters in upper and lower case. The text font and size shall produce an 80 column by 25 line display, and each character shall be displayed in any of 16 colors, selected by the user. The symbols shall consist of any custom symbols that expedite preparation and interpretation of the graphic. The symbols shall be displayed in the same size as the text in any of 16 user-selected colors. The lines shall consist of straight-line segments in any orientation, in either of two widths, single or double, and in any of 8 user-selected colors. The areas shall be definable in a consistent manner and be displayed in any of eight user-selectable colors.

b. Represent walls, doors, and miscellaneous objects on maps of the interior areas. Represent fences, gates, roads, and miscellaneous barriers and objects on maps of the interior areas.

c. Allow the user to depict the location of each sensor in the remote area using defined, unique, and easily identifiable graphic symbols. The display shall automatically depict the status of each sensor in the remote area using color coding of the sensor symbols as follows:

Steady green indicates SECURE operation (reset and no-alarm),
Steady yellow indicates ACCESS,
Flashing red indicates unacknowledged alarm,
Steady red indicates acknowledged alarms,
Steady gray indicates the sensor is shunted or masked.

d. Allow the user to depict the location of each response device in the remote area using defined, unique, and easily identifiable graphic symbols. The display shall automatically depict the status of each response device in the remote area using color coding of the symbols as follows:

Green indicates SAFE,
Steady Yellow indicates ARMED,
Steady Red indicates FIRED.

e. Automatically display the map of remote area in alarm, upon receipt of an alarm in that area, or upon operator request.

f. Provide storage media interface and functions that permit the duplication of all remote area graphics to removable media for backup and secure storage, and permit the regeneration of an individual or of all remote area graphics from the removable media used for backup.

g. Contain an editor for user preparation and editing of individual remote area graphics that can be easily generated and that provides a means for easily linking icons to sensors, provides copy and delete functions for entire remote area graphics, can be learned in a two hour period by a person familiar with at least one commercially available graphics software product. The editor shall also provide for producing a standard remote area graphic, making a single character

change to an existing graphic, and enabling lines to be easily and accurately aligned and connected.

h. Have the additional capability for a site-specific graphic representation (or scale map) of the complete system, to include all remote areas, RSMs, and the PMC area. The objective of this display is to provide the operator with a geographic perspective representation of remote area alarms with respect to the entire site to aid in assessing the intrusions and dispatching the response force. The PMC shall provide the maintainer the capability to generate a custom map of the entire site, including the PMC area, RSM areas, all remote areas, buildings, prominent terrain, roads, and any other significant, site unique features. The user shall have the capability to assign defined, unique, and easily identifiable symbols for each remote area, which indicate remote area status using the following color code for the status of the remote areas: (NOTE: Indicators for sensors are not permitted due to the scale of the maps.)

Steady green indicates SECURE operation (all sensors reset and no alarm and no sensors in ACCESS),
Steady yellow indicates ACCESS of one or more sensors,
Flashing red indicates at least one unacknowledged alarm,
Steady red indicates all alarms acknowledged.

i. Share the remote area graphic display. The operator shall have controls to select either a display of the geographic map or the individual remote area graphics. The first alarm, in an empty alarm queue, shall automatically cause the remote area graphic, in alarm, to be displayed. Subsequent incoming new alarms or status changes shall not cause the display to change until the operator manually selects another display. The graphics shall update within 0.5 seconds after any status change.

3.4.2.1.9 System Data Storage.

The PMC shall use an operating system and have sufficient storage capacity and processing speed to meet the requirements of this performance specification. Hardware and software incorporated in the PMC shall be state-of-the-art programs and devices that can reasonably be expected to be commercially supportable during the next five to seven years. The system shall have the capability to continuously and automatically store system configuration, system status, all operator actions, all periods of maintenance, and all alarm data with corresponding date and time of day into nonvolatile storage. The PMC shall be capable of selectively retrieving and printing the stored data in user-selected formats by date, time period, and type of data while on-line. The operator shall have no control of data storage. Access to replacing, printing, or backing up the historical data shall be restricted to the appropriate access level of personnel by key lock, password or other control. Provisions shall be available to allow one (1) month storage of archive data before the data must be downloaded to a permanent storage media. The system shall generate a status display message before the capacity of the data storage is reached. The message shall be generated in adequate time to replace the storage media or backup the stored data before overwriting occurs.

3.4.2.1.10 Uninterruptible Power Supply Functional Requirements.

The Uninterruptible Power Supply (UPS) shall:

a. Operate on either of the following nominal voltages and frequencies, depending on available facility power:

   (1) 120/208/240 Vac, 60 Hz,

   (2) 220 Vac, 50 Hz.

b. Provide converted facility power at the levels required by one PMC during normal operation. The UPS may be an integral part of the PMC or a separate item.

c. Starting with a full charge, provide battery backup capable of supplying power to the PMC

during facility power interruptions, for a minimum of eight hours duration, at the lowest specified operating temperature.

d. Automatically switch to backup power, upon loss of primary power, and revert when the power returns without interruption or degradation to the functioning of the PMC.

e. Be sufficiently recharged within twelve hours, after return of normal facility power, to provide power through another eight-hour facility power interruption.

f. Provide discrete output(s) indicating the status of internal tamper switches.

g. Provide discrete output(s) indicating the status (absence or presence) of primary AC power.

h. Monitor the battery voltage. If an overcharging condition at the battery terminals is measured, the primary AC supply and battery charging circuit shall be disabled and the UPS shall operate from the battery. If an under-voltage condition at the battery terminals is measured while operating from the batteries, the positive battery lead shall be opened to prevent excessive discharge. The battery lead shall be automatically reapplied after return of primary AC power. If a DC supply output exceeds or drops below a safe operating level, indicating a DC supply failure, both the primary AC and battery shall be disabled.

i. Be capable of sustaining momentary overloads of 125% of rated voltage for up to 10 minutes, and sustaining surges of 150% of rated capacity for 10 seconds.

j. Provide EMI, transient, and surge protection in accordance with paragraph 3.11 to prevent damage to equipment from lightning and other conducted electrical disturbances or, to localize damage in easily repairable low-cost components.

k. Operate in the interior controlled environment.

l. Be either internal, free-standing, or wall-mountable.

m. Provide the capability to manually switch from primary to battery power as a maintenance function, and to manually bypass the UPS.

3.4.2.1.11 CCTV Interfaces.

The PMC interfaces for the CCTV system are described below. The CCTV characteristics are specified in ICIDS-PS-0601.

a. Interface with a switching matrix controlling groups of 4 cameras up to a total of 128 cameras.

b. The operator interface shall be the CCTV control device, and visual presentations via the TV monitors. Controls for the CCTV system shall be integrated into the operator input device to allow manual operator-triggered, as well as automatic alarm-triggered, camera selection onto any of the four monitors. The alarm-triggered camera selection shall be effective only for the first alarm into the alarm queue; in the case of multiple alarms, the video for subsequent alarms must be manually selected.

c. The PMC system shall interface directly with the CCTV equipment and provide commands to the video switching matrix. The PMC shall process commands, perform data conversions to meet component interfaces, and output commands to CCTV components. The PMC shall output the identification of each alarmed remote area to the CCTV equipment within 3.0 seconds of the sensor alarm in order to make video assessment available to the operator not more than 1.0 second after the alarm is displayed on the PMC.

d. The PMC shall provide the capability, and provide sufficient memory and programmability, for implementation of an automatic mode of operation such that a single alarm at the monitor shall cause a display of up to four camera inputs from the alarmed remote area.

3.4.2.1.12 Physical Characteristics.

All components, subsystems, and subassemblies shall be readily accessible for maintenance. All enclosures shall be lockable. The operator interfaces shall be ergonomically situated for easy access, by the operator, to all controls and displays. The PMC shall be modular to permit ease of assembly, maintenance, and installation. All modules shall be capable of passing through a doorway 81 centimeters wide by 193 centimeters high.

3.4.2.2 Remote Area Data Collector (RADC).

3.4.2.2.1 Description.

RADCs are remote area items that interface sensors, sensor stimuli, response devices, Entry Control Equipment (ECE), CCTV components, and tamper devices with the PMC. Sub-RADCs are remote area items that interface sensors, sensor stimuli, CCTV components, and ECE devices with RADCs. Each RADC shall be capable of interfacing with a minimum of five (5) sub-RADCs. RADCs and sub-RADCs shall be available in various configurations to satisfy the requirements of installations worldwide. Table 1 is a summary of RADC and Sub-RADC requirements.

Table 1: RADC Configurations

RADC TYPE	VOLTAGE	NO. OF SENSORS (1)	ECE I/F (2)	KEYPAD I/F (2)	MODEM (2)	RESP DEVICE I/F (2)&(3)
INTERIOR RADC	12 Vdc	4 min 32 max	YES	YES	YES	YES
INTERIOR SUB-RADC	12 Vdc	4 min 32 max	YES	YES	NO	NO
EXTERIOR RADC	12 Vdc	4 min 32 max	YES	YES	YES	YES
EXTERIOR SUB-RADC	12 Vdc	4 MIN 16 MAX	YES	YES	NO	NO

(1) A minimum of four sensor inputs with capability of additional sensor inputs in increments, up to a maximum

of 32 sensor inputs.

(2) “YES” means required. “NO” means not required.

(3) A minimum of four relay outputs or four response device outputs is required. The number of outputs increase in increments, to a maximum of 32 total outputs.

3.4.2.2.1.1 Interior RADCs.

Interior RADCs shall be available to interface with Entry Control Equipment (ECE), keypad, variable numbers and types of sensors, sensor stimuli, response devices, and CCTV, all individually resolvable. Sub-RADCs need not interface with response devices, but must have relay outputs and be capable of operating with a keypad. Interior RADCs shall be available configured as follows:

a. A minimum of four sensor inputs, with a capability of additional sensor inputs in increments up to a maximum of 32 sensor inputs. Sub-RADC requirements are identical, as shown in Table 1.

b. Ability to communicate directly with the PMC for both high security and regular remote areas. Sub-RADCs need only communicate with RADCs.

c. Sub-RADCs shall have the capability to act as slaves to, and communicate with, other RADCs.

d. A capability to provide +12 VDC to all connected off-the-shelf commercial sensors.

e. A minimum of four relay outputs, or four response device outputs, with a capability of additional relay/response outputs in increments up to 32 total outputs.

3.4.2.2.1.2 Exterior RADCs.

Exterior RADCs shall be available to interface with Entry Control Equipment (ECE), keypad, variable numbers and types of sensors, sensor stimuli, CCTV components, and response devices, all individually resolvable. Sub-RADCs need not interface with response devices, but must have relay outputs. Exterior RADCs shall be available configured as follows:

a. A minimum of four sensor inputs, with a capability of additional sensor inputs in increments up to a maximum of 32 sensor inputs.

b. Capability to communicate directly with the PMC for both high security and regular remote areas. Sub-RADCs need only communicate with RADCs.

c. Sub-RADCs shall have the capability to act as slaves to, and communicate with, other RADCs.

d. Operate in an exterior environment.

e. Four relay outputs, or four response device outputs, with a capability of additional relay/response outputs, in increments up to 32 total outputs.

3.4.2.2.2 PMC Interface.

All RADCs shall communicate all status changes and commands with the PMC, in accordance with paragraph 3.4.2.1.3.

3.4.2.2.3 RSM Interface.

If the system configuration accommodates an interface between the RSM and the RADCs, the data to be exchanged over this interface shall be sufficient to meet the RSM performance requirements of paragraph 3.4.2.3.

3.4.2.2.4 DAS Interface.

All RADCs and sub-RADCs shall interface with a DAS for increased data transmission security, as described in paragraph 3.4.2.5.

3.4.2.2.5 Interior Sensor Interfaces.

All interior RADCs and sub-RADCs shall:

a. Interface with commercial interior sensors with the sensors being individually resolvable, and with response devices Sub-RADCs need not interface with response devices. Provide an interface to tamper switches associated with the sensors.

b. Communicate to the sensors over a minimum distance of 150 meters.

c. Provide power to all connected sensors.

d. Operate over a dedicated hardwired link.

e. Support sensors having relay contacts as an alarm output or solid state equivalents, either normally open or normally closed.

f. Provide a sensor stimulus activation output for each sensor. This output shall be activated by a self-test command from the PMC, RSM, or locally from the RADC maintainer interface. The stimuli activation output shall be a relay or voltage output that shall turn on to activate the sensor stimuli and remain on for a maximum of 8 seconds. This output shall then turn off within one second after the associated sensor alarms. For SCIF areas, the maximum on period shall be limited to 1 second. Salient characteristics for the sensor stimuli are detailed in the individual sensor PES. The RADCs are not required to provide power to the sensor stimuli.

g. Provide supervision of the lines to the sensors to detect tampering, such as shorting or cutting. Current, voltage, impedance monitoring or other effective techniques may be used.

h. Provide EMI, transient, and surge protection on all sensor interface lines, in accordance with paragraph 3.11.

i. When communication is lost between the RADCs and remote area devices (e.g., sensors), a tamper, or other distinct alarm, shall be annunciated at the PMC and/or, the RSM.

3.4.2.2.6 Exterior Sensor Interfaces.

All exterior RADC and sub-RADC sensor interfaces shall be the same as the interior sensor interfaces described in paragraph 3.4.2.2.5, above, with the following exceptions:

a. The minimum operating distance shall be 1000 meters.

b. Need not provide power to the exterior sensors.

c. Sub-RADCs need not interface with response devices.

3.4.2.2.7 Response Device Interface.

All RADCs shall interface to response devices. The response devices shall be triggered (activated) under direct command from the PMC through the RADC. The RADCs shall provide the capability to enable, disable, activate, and deactivate response devices through PMC operator command. The enable command shall be used to place the response device into a ready state (armed). The disable command shall return the response device to a quiescent state (unarmed). The activate command shall latch the response device on, and shall be effective only if all required conditions cited below are met. The deactivate command shall return the response device to the quiescent state and reset the activate latch. A response device shall not be activated unless all of the following conditions are present: 1) the response device has been previously enabled; 2) the RADC is in the SECURE mode of operation; 3) a valid alarm is active in the same remote area; and 4) the response device activate command has been received. The response device interface shall also:

a. Provide a minimum of four response device channels in the RADCs.

b. In the interior RADCs, communicate to the response devices over a minimum distance of 150 meters.

c. In the exterior RADCs, communicate to the response devices over a minimum distance of 1000 meters.

d. Operate over a dedicated hardwired link.

e. Provide a response device status input to support response devices having a normally open or normally closed relay contact output that indicates the ready or spent status of the device.

f. Provide response device enable and activate output relays, either normally open or normally

closed contacts (Form C), with a minimum contact rating of 0.25 amperes at 24 Vdc.

g. Support response devices having a tamper switch or relay tamper alarm output, either normally open or normally closed contacts.

h. Provide line supervision to detect line tampering, such as shorting or cutting. Current, voltage, or impedance monitoring, or other effective techniques may be used.

i. Provide EMI, transient, and surge protection on all response device interface lines, in accordance with paragraph 3.11.

3.4.2.2.8 ECE Interface.

All interior RADCs shall interface as follows:

a. To Entry Control Equipment (ECE), as specified in ICIDS-PS-0602, for receiving and displaying entry control information (e.g., entry approved, entry denied alarms, and tamper information). Upon entry approval, sensor alarms generated during ingress shall be inhibited during a variable (0-90 second) delay. For SCIF applications, the ingress delay shall not exceed 30 seconds. The ingress delay provides an authorized user adequate time to enter the area and switch the RADC from the SECURE to the ACCESS mode of operation.

b. As a user option, when an entry approved message is received from an attached ECE, the RADC status shall be changed from SECURE to ACCESS. The alternate user option is to require the mode change to be performed manually by a key switch or a keypad. This function may be implemented at the RADC or the PMC. The RADC status change shall be displayed, but require no operator action to acknowledge or reset. The RADC identity, status change and time of each ECE event shall be retained in the non-volatile system data storage and the Personal Identification Number (PIN)/badge number and

badge holder identification information shall be retained either locally at the ECE or at the PMC.

c. Prohibit the ECE, installed outside the SCIF, from automatically changing the RADC mode of operation to ACCESS, SECURE, OFF-LINE, or from shunting any sensors within the SCIF without continuous annunciation of the shunted sensors at the PMC. Additionally, the identity of ECE users in SCIFs shall not be divulged to the console operator, except by some coded identifier.

d. PMC interface shall be accomplished either directly to the PMC or through a RADC located in the vicinity of the PMC.

e. Intrusion alarms shall have a higher priority than ECE.

3.4.2.2.9 RADC and Sub-RADC Power Supplies.

All RADC and sub-RADC power supplies shall:

a. Provide the RADC or sub-RADC and all attached sensors with operating power. The minimum load capacity of the power supply shall be 0.25 ampere @ 12 Vdc for 8 attached sensors, plus the power requirement of the RADC or sub-RADC. If the RADC sensor capacity is greater than 8, then the supply is required to provide a corresponding additional power at a level of approximately 30 milliamperes per sensor.

b. Operate on either of the following nominal voltages and frequencies, depending on available facility power:

(1) 120/208/240 Vac, 60 Hz.
(2) 220 Vac, 50 Hz.

c. Include battery backup, capable of supplying sufficient power to the RADC or sub-RADC and attached interior sensors, during facility power interruptions for a minimum of 8 hours at the lowest specified temperature.

d. Automatically switch to backup power, upon loss of primary power, and revert when the primary power returns, without interruption or degradation of the functioning of the RADC or sub-RADC and the connected sensors.

e. The battery shall be sufficiently recharged, within 12 hours after the return of primary power, to provide power through another 8 hour primary power interruption.

f. Be located within the RADC or sub-RADC enclosure.

g. Provide discrete output(s) indicating the status (absence or presence) of primary power.

h. Continuously monitor the battery voltage. If an over-voltage condition is measured at the battery terminals, the primary AC supply and battery charging circuit shall be disabled and operation shall continue on the battery. If an under-voltage condition is measured at the battery terminals while operating from the battery, the positive battery lead shall be disconnected to prevent excessive discharge. The battery lead shall be automatically reapplied after return of primary AC power. If a DC supply output out-of-tolerance condition is measured, indicating a power supply failure, both the primary AC and battery shall be disabled. Any power loss shall be reported to the PMC.

i. Be capable of sustaining momentary overloads of 125% of rated capacity for up to 10 minutes, and sustaining surges of 150% of rated capacity for 10 seconds.

j. Include EMI, transient, and surge protection, in accordance with paragraph 3.11, to prevent damage to equipment from lightning and other conducted electrical disturbance, or to localize damage to easily repairable, low-cost components.

k. Operate in either or both interior and exterior environments.

l. Include a capability to manually switch from primary power to battery power as a maintenance function, and to manually bypass the battery.

m. Include an illuminated indication of the power source in use (i.e., AC or DC). The indicator shall change color or flash when operating off the battery.

3.4.2.2.10 RADC/Sub-RADC Maintainer Interface.

All RADCs and sub-RADCs shall provide a means to allow maintenance within the remote area. ON-LINE maintenance shall be utilized unless specific system requirements or safety factors preclude implementation. Maintenance access shall be through a key-locked door. A password or other unique identifier shall be required for access to the maintenance mode. Conduct of maintenance activities shall place the RADCs and sub-RADCs into a maintenance mode, which shall be continuously signaled to the PMC for the duration of the maintenance activity. The RADCs and sub-RADCs shall provide a means to store and display an historical file of the last ten alarms since these devices were last placed into the SECURE mode of operation. A RADC installed in a SCIF shall not have the capability to be remotely diagnosed.

a. All RADCs and sub-RADCs shall have a Built-In Test (BIT) capability to enable maintenance personnel to perform tests of all connected remote area devices. The BIT shall be able to differentiate which connected device(s) are asserting a tamper or communication line failure condition. The BIT shall also provide for fault isolation to the Line Replaceable Unit (LRU).

b. A capability shall also be provided to configure the RADC and sub-RADC address, ingress and egress delay times, and all other configuration actions necessary to properly implement the requirements of these devices. The configuration attributes may be assigned through the maintainer interface or via the PMC, except in the case of SCIFs where remote programming is prohibited.

c. All RADCs and sub-RADCs shall provide a walk-test mode that shall be selectable only while the maintenance mode is active. This mode allows the

maintainer to conduct manual walk-tests of the sensors in the remote area. While active, the walk-test mode shall annunciate all sensor and tamper alarms for the duration of the alarm condition and be silent when no alarm is active.

3.4.2.2.11 ACCESS/SECURE Switch/Keypad Interface.

The RADC and sub-RADC shall provide switch/keypad interface as follows:

a. Include an integral, enclosure mounted, key operated, two-position switch for local ACCESS/SECURE mode selection. The RADC and sub-RADC shall monitor this switch for position and report the mode to the PMC. Any mode changes from ACCESS to SECURE shall automatically initiate a self-test of all remote area sensors within 90 seconds after the mode change. It shall not be possible to inhibit tamper or duress alarms in either mode of operation.

b. Provide a capability for bypassing the ACCESS/SECURE switch, thereby removing the capability for local mode changes. With this capability, mode changes shall only be possible when commanded from the PMC or RSM. This capability shall support the implementation of two-person rule at the PMC and/or RSM for ACCESS/SECURE/OFF-LINE mode changes.

c. Provide a keypad as an alternative to the ACCESS/SECURE switch, and accept the output of a keypad or entry control equipment that can uniquely identify an authorized user. When the authorized user enters his unique PIN, or is otherwise uniquely identified (i.e., smart card or biometric device), the RADC or sub-RADC shall automatically change modes from ACCESS to SECURE or SECURE to ACCESS. The user’s identity shall be logged at the PMC or RSM, as applicable. Remote mode changes (e.g., from the PMC or RSM) are expressly prohibited for RADCs used in SCIFs and must be disabled when this mode of operation is selected at initial configuration. Entry control equipment within the SCIF may be used for the mode change, provided that the mode change

process is handled entirely within the SCIF and is completely disassociated from normal entry control activities.

d. When in the SECURE mode of operation, the RADC or sub-RADC shall report all sensor and tamper alarms and be capable of enabling, disabling, activating, and deactivating response devices. Video assessment devices shall be capable of being activated when in the SECURE mode of operation.

e. When operating in the ACCESS mode, all response device activation and sensor alarm annunciation shall be inhibited, except for sensors not ACCESS INHIBITED at installation. Video cameras shall not be capable of being activated when in the ACCESS mode of operation,

f. When the ACCESS INHIBIT mode of sensor operation is implemented at the PMC, RADC or sub-RADC at installation, sensor(s) so configured are inhibited from being ACCESSED. These selected sensors remain in the SECURE mode and all alarms from these sensors shall be reported and displayed, at the PMC and RSM, regardless of the mode of operation.

3.4.2.2.12 Physical Characteristics.

The RADC and sub-RADC enclosures shall have a key-locked door. The enclosure shall be designed to meet the specified environmental conditions. The enclosures shall be metallic and meet the requirements of a NEMA 3R enclosure as specified in NEMA 250. Interior structural components shall have the strength and rigidity to conform to the conditions specified in UL 1076, Section 7. The door and any removable covers shall be provided with door/cover operated corrosion-resistant tamper switches. Enclosure construction shall ensure battery safety. The enclosure shall be capable of being mounted on a horizontal surface, wall, or post.

3.4.2.3 Remote Status Monitor (RSM).

3.4.2.3.1 Description.

The RSM shall be capable of two modes of operation: 1) a display-only mode wherein all, or user selected portions, of the ICIDS status is displayed; and 2) a CCD mode wherein the control of all, or a user selected portion, of the system shall be transferred from the PMC to the RSM. The RSM shall provide an input device to enable the operator to interact with the system when in the CCD mode.

The major functional areas of the RSM are:

a. Command, Control and Display (CCD)

b. Status display

c. Operator interface

d. Interconsole interface (RSM to PMC)

e. Enrollment

3.4.2.3.2 Command, Control and Display Processing.

The RSM shall:

a. Provide two modes of operation, selectable at the user's option:

(1) Command, Control and Display (CCD) Mode. The RSM shall provide a mode (selectable via key switch or password) in which it is capable of assuming command and control of all or part of the connected RADCs from the PMC, and releasing control back to the PMC automatically or upon command. The RSM shall provide the capability, upon configuration at the user's option, to assume control of remote areas assigned to it. In this operating mode, the RSM shall be capable of performing all of the command and control functions of the PMC as specified in paragraph 3.4.2.1.3, except as excluded in paragraph 3.4.2.3.1. A typical application of an RSM, in this mode of operation, would be a facility which assumes

control of the remote areas within its perimeter during the working hours of the day, and relinquishes control to the PMC at night.

(2) Display-Only Mode. The RSM shall provide a display-only mode in which the operator has no control over system functions, except to acknowledge or concur with two-person rule requests. In this mode, the RSM shall receive and display all, or user-selected portions, of the system status being displayed at the PMC (e.g., mimic the PMC status display). The RSM shall permit the operator to monitor the actions of the PMC operator.

b. Monitor all PMC, RSM, and remote area communications and data flow, as the system architecture dictates.

c. Provide the communication interfaces to connected RADCs/sub-RADCs and/or PMCs with the following capabilities:

(1) Send and receive data by one or more of the following separate interfaces and data link subsystems. The choice of data link shall be made prior to installation and shall not limit any system performance nor preclude the use of the DAS. The RSM is required to support any combination of the following data links, selected by the user:

(a) Interfaces with continuous metallic wire pairs. Salient characteristics typical of metallic pairs are summarized at Attachment 1 to this Performance Specification. This hardwired link shall be compatible with the DAS, whether internal or external.

(b) A commercial RF/microwave data link may be specified, by the Government, prior to installation for some or all remote areas or PMC-to-RSM data communication. It shall be compatible with the metallic wire pair

interfaces at the PMC, RSM, and RADC, and shall also be compatible with the DAS, whether integral or external.

(c) A commercial fiber optic communication interface is an option to be specified, by the Government, prior to installation for some, or all, remote areas or PMC-to-RSM data communication. The transmit/receive circuitry, which interfaces to the fiber cable, may be internal (e.g., replaces hardwired modem) or external (e.g., connects to PMC hardwired output). It shall be compatible with the PMC, RSM and RADC data communication interfaces. The fiber optic communication interface shall utilize fiber optic cable and components as specified in CEGS-16768, Fiber Optic Data Transmission Media for Security Systems.

(2) Execute error detection and line supervision processes in order to monitor, detect, and report the loss of line integrity of the communication links.

(3) The RSM-to-PMC and RSM-to-RADC links (as architecture dictates) shall be capable of operating up to 16 kilometers without repeaters or relays, regardless of the type of data link used. This communication interface is required to be supervised, and communication faults annunciated.

(4) Receive system status information including:

(a) Sensor alarms

(b) Sensor tamper

(c) RADC status including ACCESS/SECURE/OFF-LINE mode

(d) RADC tamper

(e) RADC power supply fail alarms

(f) PMC status

(g) Response device status

(h) Remote area configuration

(i) Self-test commands and results

(j) Entry control equipment data (e.g., entry approved/denied). The RSM shall be notified of any shunted sensor.

d. Monitor the tamper conditions for the PMC, RSM and power supply.

e. Monitor AC power status for the RSM.

f. Monitor operator input device data (commands, requests, etc.).

g. Display system configuration data, including date and time of most recent system configuration changes.

h. Provide for orderly shutdown and restart whenever components are replaced, or have lost information, because of power failure or component failure.

i. Provide for automatic nonvolatile data storage for historical data, system configuration data, and system status (e.g., configuration tables, databases, periods of maintenance, sensor shunting). The operator shall have no control of data storage, and access to replacing, or backing up the historical data is restricted to personnel with the appropriate level of access.

j. Have provisions for automatic storage of system configuration data and automatic reinitialization of system configuration from data storage after any system outage (i.e., power outage or system maintenance downtime). Reinitialization time, from power on until full system operation, shall not exceed five minutes.

k. Provide sufficient reserve capacity in main memory to accept future software changes and

system expansion. Main memory is memory from which stored programs are executed and within which program data, and input/output operations are stored.

l. Provide for both a manual and an automatic self-testing of the system with the capability for user definable and programmable parameters at installation. These parameters shall include duration of test, number of tests per a given time period. The interval between automatic tests shall be randomized. Intentional alarms generated on a specific device, while under self-test, shall be suppressed. Any valid alarm, such as intrusion, tamper or duress (other than an intentional alarm), generated during a self-test, shall cause the self-test to terminate and the alarm shall be annunciated. The results of all self-tests shall be recorded in the system data storage. Only self-test failures shall be annunciated at the RSM(s) status displays. Any mode change from ACCESS to SECURE shall automatically initiate a self-test of the remote area equipment within 90 seconds after the mode change.

m. Provide EMI, transient, and surge protection on all external interface lines, in accordance with paragraph 3.11.

n. Provide for two processes to change the ACCESS/SECURE mode of operation of a RADC for an individual sensor or for the entire RADC: 1) from the RSM in CCD mode, or 2) from the RADC. The functional requirements of the ACCESS and SECURE modes are as described for the PMC.

The RSM in the CCD mode shall provide the operator the capability to change the ACCESS/SECURE/OFF-LINE mode of a remote area or sensor by entering a command at the keyboard (except for SCIF areas where remote commanded ACCESS/SECURE/OFF-LINE is prohibited or locked-out at installation). The two-person rule requirements apply to commanded ACCESS/SECURE/OFFLINE mode changes when so configured at installation.

The RSM in both the CCD and Display-Only modes shall monitor and continuously display the mode of operation of the sensors and RADCs. SECURE mode shall be indicated by green color for icons, indicators and graphics. ACCESS shall be indicated by yellow color. Alarms shall be displayed in red.

o. Provide a unique, audible alarm that is activated to alert the operator when any alarm displayed at the PMC remains unacknowledged by the PMC operator for a preset time. The audible alarm is in addition to the visual alarm displayed on the RSM status display. The time limit is adjustable as a maintenance function and is set at initial RSM configuration.

3.4.2.3.3 Operator Interface.

The RSM operator interface shall provide:

a. An operator input device (e.g., keyboard, mouse, etc.). While the RSM is in CCD mode, the operator input device shall provide all of the functions available to the PMC operator, as previously described. The input device shall provide controls which:

(1) Aid display interpretation

(2) Select alternate display formats

(3) Silence the audible indicator when an alarm is acknowledged

(4) Clear the display of data pertaining to status changes which have been acceptably processed by the console operator

(5) Adjust the auditory signal volume to be heard above any expected ambient noise

While the RSM is in display-only mode, the operator input device and all command and control functions shall be disabled.

b. A maintenance input device, such as a keyboard or other device, to permit a maintenance technician to perform the following maintenance activities. Unauthorized access to the maintenance input device shall be protected against by a mechanical and/or electrical lock (e.g., password, locked panel, etc.). The maintenance tasks shall include:

(1) configuration modifications, both at initial installation and as required, including setting the time and date,

(2) system initialization and reinitialization, which shall be independent of the PMC and its operator,

(3) system self-diagnostics (shall be disabled for RADCs installed in SCIFs), and

(4) selecting the portion of the PMC display to be displayed at RSM (if accomplished at RSM).

c. A status display. Shall utilize a visual display, in color, of at least 48 centimeters diagonal in size with a minimum resolution of 1280 by 1025 pixels. While the RSM is in CCD mode, the status display shall function as described herein for the PMC.

While the RSM is in display-only mode, the status display shall:

(1) display all, or selected portions, of the host PMC system status, independent of the PMC (i.e., the RSM operator may autonomously select any display, regardless of the display currently selected at the PMC),

(2) reject status data explicitly disabled during RSM initialization or configuration, and

(3) display data in a format similar to the PMC status display; this shall include video and audible indicators. However, the format

shall be modified such that the RSM operator can monitor keyboard responses by the PMC operator.

3.4.2.3.4 Interconsole Interface.

The RSM shall:

a. Communicate (directly, if architecture dictates) with the PMC to receive all, or selected portions, of the system status and all PMC operator actions for use by the RSM (depending on operating mode).

b. Interface with a DAS to encrypt system data for use by the RSMs. Disruption or loss of these communication lines shall be annunciated at the PMC and RSMs as line security alarms.

3.4.2.3.5 Uninterruptible Power Supply.

The RSM UPS shall perform in accordance with the requirements for the PMC UPS described in paragraph 3.4.2.1.10.

3.4.2.3.6 System Data Storage.

The RSM shall use an operating system and have sufficient storage capacity and processing speed to meet the requirements of this performance specification. Hardware and software incorporated in the RSM shall be state-of-the-art programs and devices that can reasonably be expected to be commercially supportable during the next five to seven years. The system shall have the capability to continuously and automatically store system configuration, system status, all operator actions, all periods of maintenance, and all alarm data with corresponding date and time of day into nonvolatile storage. The RSM shall be capable of selectively retrieving and printing the stored data, in user selected formats, by date, time period, and type of data, while on-line. The operator shall have no control of data storage, and access to replacing, printing, or backing up the historical data shall be restricted to the appropriate access level of personnel by key lock, password or other control. Provisions shall be available to allow a one (1) month storage of archive data before the data must be downloaded to a permanent storage media. The system shall generate a status display message before the capacity of

the data storage is reached. The message shall be generated in adequate time to replace the storage media or backup the stored data before overwriting occurs.

3.4.2.3.7 Physical Characteristics.

The RSM shall be modular to permit ease of assembly, maintenance, and installation. All modules shall be capable of passing through a doorway 81.25 centimeters wide by 193 centimeters high. The RSM and UPS shall both be free-standing, floor-mounted. The UPS shall also be capable of being mounted, remotely, up to 15.25 meters from the RSM.

3.4.2.3.8 Closed-Circuit Television (CCTV) System Interface.

The RSM does not require an interface with the CCTV.

3.5 Data Authentication System (DAS).

3.5.1 Description.

The Data Authentication System (DAS) shall provide secure data communication using National Institute of Standards and Technology (NIST) validated Data Encryption Standard (DES) encryption as specified in FIPS-46-3 and conforming to the requirements of FIPS-PUB-140-1, for data communications between PMC-to-RSM, PMC-to-RADC, and RSM-to-RADC (if architecture dictates). The DAS may be internal or external, and may be optionally installed within the PMC, RSM, and RADC enclosures. In either case, the DAS shall be physically compatible and electrically interoperable with the PMC, RSM and RADC hardwired data links, and other system components, including the optional fiber optic communication interface, and the optional RF/microwave data link. It shall derive operating power from existing power source(s). The DAS shall provide the capability to remotely install or change the RADC encryption key.

3.5.2 DAS Interfaces.

The Data Authentication System (DAS) interfaces shall consist of external interfaces defined in the following paragraphs:

a. DAS communication interfaces. The DAS shall provide optional data encryption capability for applicable PMC, RSM, and RADC communication channels whether hardwired, RF/microwave, or fiber optic. The DAS equipment shall receive an

encryption key variable from a key carrier, in the case of local keying, or from the host console or remote keying device, in the case of remote keying capability.

b. DAS electrical interfaces. The DAS shall derive electrical power from the PMC, RSM, or RADC, as applicable. Power consumption shall be compatible with host component requirements for power consumption, backup power capability, and thermal design. The DAS shall provide an interface(s) compatible with the hardwired, RF/microwave and fiber optic data links.

c. DAS physical interfaces. The DAS components shall be modular to allow for optional installation within the PMC, RSM, or RADC for site specific applications. The DAS components commonality in design and form factor shall be maximized in the interest of interchangeability and inventory cost reduction. The form factor and weight of DAS components shall be consistent with specified modularity and redundancy requirements and with space limitations within the PMC, RSM, and RADC enclosures. Each DAS unit shall be of modular form to allow configuration for either encrypted or non-encrypted operation.

3.5.3 DAS Functional Characteristics.

The DAS shall provide data encryption for the specified communication channels. A DAS secure communication channel will require installation of a DAS device at each end of the communication link (e.g., within the PMC and within the RADC). The DAS shall provide sufficient capacity, flexibility and redundancy to allow any or all eligible communication channels of a PMC, RSM, or RADC to operate simultaneously in the encryption mode.

3.6 Radio Frequency (RF)/Microwave Communication Network

3.6.1 Description.

The RF/Microwave communication network shall be an option for the PMC, RSM, and RADC in place of any or all of the metallic wire pairs (hardwired lines).

3.6.2 Interface Requirements.

The RF/Microwave communication network shall provide the same interface specified for metallic wire pairs and be installed in place of the hardwired communication link at the user's determination.

3.6.3 Functional Requirements.

The RF/microwave communication network shall function under the PMC, RADC, and RSM program control and conform to the specified functional requirements for metallic wire pairs.

3.7 Fiber Optic Communication Interface.

3.7.1 Description.

The fiber optic communication interface shall be a user option for interfacing the PMC, RSM, and RADC in place of any or all of the metallic wire pairs (hardwired lines).

3.7.2 Interface Requirements.

The fiber optic communication interface shall provide the same interfaces specified for metallic wire pairs, described herein.

3.7.3 Functional Requirements.

The fiber optic communication interface shall function under the PMC, RADC, and RSM program control and conform to the specified functional requirements for metallic wire pairs, described herein. The PMC, RSMs and RADCs shall provide all necessary data communication circuitry to interface to fiber optic cable and components, per guidance contained in CEGS-16768.

3.8 Human Factors Engineering (HFE).

To facilitate ICIDS performance, Human Factors Engineering (HFE) shall ensure that detected events are easily recognized by the operator. Displays that alert the operator to events requiring a response shall be clear and complete. The HFE principles and design requirements of commercial standards shall be used as guidance to ensure the effectiveness of man-equipment interfaces (e.g., controls, indicators, and displays) and to eliminate unnecessary demands on human skill, training, and manpower.

3.9 Safety.

a. To the maximum extent possible, the components shall be composed of such materials and operate in such a fashion that neither its presence nor operation shall impair the health or safety of persons coming near or into contact with it.

b. The design shall incorporate positive methods to protect operating and maintenance personnel from accidental contact with hazards. No special clothing, training, or equipment shall be necessary for safe operation of the remote area items.

c. Special handling requirements and other safety precautions shall be conspicuously labeled. All equipment shall meet the requirements of National Electrical Code, NFPA-70 2005, and shall be in accordance with applicable UL 1076 safety standards as guidance to ensure ICIDS is safe to operate and maintain.

3.10 Environmental Requirements.

3.10.1 Natural Environment.

The components of the CCDS shall withstand environmental conditions, or combinations of, as follows:

3.10.1.1 Interior Components

3.10.1.1.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -10^{o} C and +60^{o} C.

3.10.1.1.2 Operating Conditions.

a. Temperature.

(1) For console area components, shall be able to operate, as specified herein, in any temperature between +10^{o} C and +40^{o} C.

(2) For other interior area components, shall be able to operate, as specified herein, in any temperature between 0^{o} C and $+50^{o}$ C.

b. Relative Humidity. The CCDS components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

3.10.1.2 Exterior Components

3.10.1.2.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -10^{o}C and $+60^{o}$C.

3.10.1.2.2 Operating Conditions

a. Temperature. The CCDS components shall be able to operate, as specified herein, in temperatures between -10^{o} C and $+50^{o}$ C.

b. Relative Humidity. The CCDS components shall be able to withstand relative humidity between 20% and 85% (non-condensing).

c. Rain. The CCDS exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 57.

d. Dust. The CCDS exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 58.

3.10.2 Impact and Vibration.

The CCDS components shall not be damaged and shall operate, as specified herein, when subjected to the jarring test as specified in UL 1076 section 39.

3.10.3 Vibration.

The CCDS RADCs shall not be damaged by vibration when tested, as specified in UL 639, Section 37.

3.11 Electromagnetic Interference (EMI) Control.

3.11.1 Electromagnetic Radiation.

The CCDS shall comply with the requirements of Federal Communications Commission (FCC) Part 15, Class B equipment.

3.11.2 Induced Environment.

The CCDS shall meet lightning, EMI transient and power surge requirements of UL 1076, Sections 44 and 45.

3.11.3 Lightning.

Equipment shall be protected to prevent equipment damage as a result of transients conducted into the equipment through power, communication, and/or control lines by natural phenomena such as lightning, or to localize damage in easily repairable low-cost components.

3.12 Finish.

3.12.1 Treatment and Painting.

Unless otherwise specified, the portions of the components subject to corrosion shall be cleaned, treated and painted.

3.13 Identification Plate or P/N Marking.

All components of the CCDS shall be identified with make, model/part number and serial number in accordance with UL 1076.

3.14 Workmanship.

Workmanship shall be in accordance with best commercial standards and practices as specified in UL-1076. These requirements are applicable to wiring, welding, brazing, plating, riveting, finishes, machine operations, screw assemblies, and freedom of parts from burrs, sharp edges, or any other damage or defect that could make the part (or equipment) unsuitable for the purpose intended.

4. VERIFICATION.

Verification is the process of inspection to show that the CCDS functions within the ICIDS and meets the requirements of the Performance Specification. All inspection results shall be documented in contractor prepared reports. The Government

reserves the right to perform any of the inspections set forth in this specification where such inspections are deemed necessary to ensure supplies and services conform to the prescribed requirements.

The inspection requirements, specified herein, are classified as follows:

a. Performance Verification Test (PVT-1) (see 4.2.1).

b. Performance Verification Test (PVT-2)/System Performance Verification (SPV) (see 4.2.2).

4.1 Methods of Verification.

Table 2 provides the methods utilized to accomplish verification including:

a. Contractor performed analysis (C/A)is an element of verification that utilizes established technical or mathematical models or simulations, algorithms, charts, graphs, circuit diagrams, or other scientific principles or procedures to provide evidence that the stated requirements were met. An "x" in the C/A column of Table 2 indicates that details of the analysis performed by the Contractor shall be provided in the Test Plan and the analysis shall be included in the Test Report.

b. Contractor performed examination (C/E) is an element of verification and inspection consisting of investigation, without the use of special laboratory appliances or procedures, of items to determine conformance to specified requirements. Examination is generally nondestructive and typically includes the use of simple physical manipulation, mechanical and electrical gauging and measurement. An "x" in the C/E column of Table 2 indicates that the Contractor conducted examination shall be included in the Test Plan, and the results of the examination shall be included in the Test Report.

c. Contractor performed test (C/T) is an element of verification and inspection which generally denotes the determination, by technical means, of the properties or elements of items, including functional operation, and involves the application of established scientific principles and procedures. An "x" in the C/T Column of Table 2 indicates that the Contractor conducted test shall be included in the Test Plan. Details shall be provided in the Test Procedure, and the results of the tests shall be included in the Test Report.

4.2 Performance Verification Inspection.

Performance verification inspection includes:

4.2.1 Performance Verification Inspection – 1

Performance Verification Inspection – 1 includes analysis, examination, and PVT-1 of the fully integrated ICIDS-IV system consisting of at least one component of each hardware/software item. The Contractor shall conduct the test, in accordance with (IAW) Government approved test plans and procedures and using the test methods described in Table 2, to verify the ICIDS system performance.

4.2.2 Installed Performance Verification Inspection – 2

Performance Verification Inspection – 2 includes analysis, examination, and PVT-2 of the first installed ICIDS-IV system to verify performance prior to Government acceptance. Contractor generated, Government approved test plans and test procedures shall be utilized using the test methods described in Table 2 to verify acceptable system performance.

4.2.3 Installed System Acceptance Inspection

Installed System Acceptance Inspection includes analysis, examination, and System Acceptance Test (SAT) of each installed ICIDS-IV system, subsequent to the first system, to verify performance prior to Government acceptance. Contractor generated, Government approved test plans and procedures shall be utilized using the test methods described in Table 2

to verify acceptable system performance.

TABLE 2

Paragraph		C/A	C/E	C/T
3.4.1.1	To report.			x
3.4.1.2	To assess.			x
3.4.1.3	To deter.			x
3.4.1.4	System timing.			x
3.4.1.5	Tamper protection.			x
3.4.1.6	Printer	x		
3.4.2.1	Primary monitor console.			x
3.4.2.1.1	Description.		x	
3.4.2.1.2	Functional areas.			x
3.4.2.1.3	CCD Functions.			x
3.4.2.1.4	Operator interface.			x
3.4.2.1.5	Remote area communication.			x
3.4.2.1.6	Interconsole communication.			x
3.4.2.1.7	Status display.			x
3.4.2.1.8	Geographic map display.			x
3.4.2.1.9	System data storage.	x		
3.4.2.1.10	UPS.			x
3.4.2.1.11	CCTV interface.			x
3.4.2.1.12	Physical Characteristics.		x	
3.4.2.2.1	RADC Description.			x
3.4.2.2.2	PMC interface.			x
3.4.2.2.3	RSM interface.			x
3.4.2.2.4	DAS interface.			x
3.4.2.2.5	Interior sensor interface.			x

Paragraph		C/A	C/E	C/T
3.4.2.2.6	Exterior sensor interface.			x
3.4.2.2.7	Response device interface.			x
3.4.2.2.8	ECE interface.			x
3.4.2.2.9	RADC/Sub-RADC Power Supplies			x
3.4.2.2.10	RADC/Sub-RADC maintainer interface.			x
3.4.2.2.11	ACCESS/SECURE Switch/Keypad interface.			x
3.4.2.2.12	Physical Characteristics.		x	
3.4.2.3.1	RSM Description.			x
3.4.2.3.2	RSM CCD processing.			x
3.4.2.3.3	RSM operator interface.			x
3.4.2.3.4	Interconsole interface.			x
3.4.2.3.5	RSM UPS.			x
3.4.2.3.6	RSM system data storage.	x		
3.4.2.3.7	RSM physical characteristics.		x	
3.5.1	DAS functions.			x
3.5.2	DAS interface.			x
3.5.3	DAS functional characteristics			x
3.6.1	RF/Microwave comm.	x		
3.6.2	RF/Microwave interface.	x		
3.6.3	RF/Microwave functions.	x		
3.7.1	Fiber optic communication	x		
3.7.2	Fiber optic interface.	x		
3.7.3	Fiber optic functions.			x
3.8	HFE.		x	

Paragraph		C/A	C/E	C/T
3.9	Safety.		x	
3.10	Environmental Requirements	x		
3.11	EMI Control.	x		
3.12	Finish.		x	
3.13	Id Plate Or P/N Marking.		x	
3.14	Workmanship.		x	

5. PACKAGING.

Packing requirements will be specified in Section D of the contract.

6. NOTES

This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.

6.1 Intended Use.

The PMC, RADC, RSM and communication links, specified herein, are components of the ICIDS. The ICIDS will provide intrusion detection capability for DoD resources worldwide.

6.2 Definitions.

DRAFT

31 OCTOBER 2005
Revision 0

ICIDS-PS-0601

PERFORMANCE SPECIFICATION

FOR

CLOSED CIRCUIT TELEVISION ASSESSMENT EQUIPMENT

OF THE

INTEGRATED COMMERCIAL INTRUSION

DETECTION SYSTEM IV

DRAFT V2

Solicitation Number

Table of Contents

1. SCOPE.

1.1 Identification.

This Performance Specification (PS) covers the Closed Circuit Television (CCTV) assessment subsystem of the Integrated Commercial Intrusion Detection System (ICIDS).

1.2 Subsystem Description.

The CCTV subsystem functions as a part of the ICIDS to allow visual assessment of intrusion alarm sites, in near real time, at a central monitoring location. The subsystem is used to capture the scenes at the alarm sites, transmit images to the monitoring location, process the images through switching devices, and display the multiple images on multiple monitors for operator assessment. The subsystem has the capability to uniquely identify each signal from each alarm site and record it for future use.

1.3 Subsystem Overview.

There are two (2) applications of the CCTV subsystem:

1) Exterior Intrusion Alarm Sites
2) Interior Intrusion Alarm Sites

Unless otherwise specified, the requirements pertain to all applications.

2. APPLICABLE DOCUMENTS.

Section 2 of ICIDS-PS-0600 shall apply with the following additions.

The following documents of the issue in effect on the date of request for proposal form a part of this description to the extent specified herein.

2.1 Government Documents.

Military.

ICIDS-PS-0600	INSERT DATE	Performance Specification (PS) for Integrated Commercial Intrusion Detection System (ICIDS) Command, Control, and Display Subsystem (CCDS)

2.2 Non-Government Documents.

2.2.1 Electronic Industries Association (EIA).

EIA-310-D	September 01, 1992	Racks, Panels and Associated Equipment
EIA-330	November 01, 1966	Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1

2.2.2 Underwriters Laboratories.

UL 639	February 21, 1997	Standard for Intrusion-Detection Units
UL 1076	September 29, 1995	Standard for Proprietary Burglar Alarm Units and Systems
UL 1492	April 30, 1996	Audio-Video Products and Accessories

2.2.3 American National Standard Institute.

ANSI C62.41	1991	IEEE Recommended Practice for Surge Voltages

2.3 Order of Precedence.

In the event of a conflict between the text of this specification and the references cited, the text of this specification takes precedence. Nothing in this specification, however, shall supersede applicable laws and regulations unless there is a specific exemption.

3. REQUIREMENTS.

3.1 Description.

The CCTV System is to be used in conjunction with the Integrated Commercial Intrusion Detection System (ICIDS), as defined in

ICIDS-PS-0600, to allow a console operator to visually assess the causes of intrusion alarms at remote areas. The CCTV configuration described herein is intended to illustrate functional requirements only and is not intended as a design constraint. The CCTV shall make maximum use of existing components and materials and leverage existing technologies to meet or exceed the requirements of this specification. While the requirements of this specification are stated in terms of conventional equipment, innovation and application of emerging technologies should be applied where possible. Utilization of infrared cameras and unitized pan tilt zoom mounts are examples of this philosophy.

3.2 Reliability.

The CCTV equipment shall have a minimum Mean-Time-Between-Failures (MTBF) of 2500 hours for an installation with 128 video input monitor area equipment and 18,000 hours for remote area equipment (combination of camera, lens, enclosure and mounting) equipment.

3.3 Construction.

UL 1492 shall apply.

3.4 Maintainability.

3.4.1 Maintenance Support.

The Mean Time To Repair (MTTR) of any CCTV component shall not exceed 0.5 man-hours.

3.4.2 Maintenance Ratio.

The maintenance ratio for high capacity (128 video inputs) monitor area equipment shall not be more than .0004. The maintenance ratio for remote area equipment (combination of camera, lens, enclosure and mounting) equipment shall be not more than .000056.

3.5 Performance Characteristics.

All items shall either be UL listed or meet the requirements of UL standard 1410, as applicable.

3.5.1 Camera.

The video camera shall conform to EIA-330 specifications. All electronic components shall be solid state. The camera shall have a back focus. Cameras shall be capable of supporting Pan Tilt Zoom (PTZ) as required.

3.5.1.1 Signal-to-Noise Ratio.

The signal-to-noise ratio shall be not less than 46dB unweighted.

3.5.1.2 Distortion.

The camera shall comply with EIA-330.

3.5.1.3 Lens Mount.

The lens mount shall be a C-mount.

3.5.1.4 Power.

The camera shall be capable of operating on supplied facility power. Nominal voltages and frequencies are: 1) 120/208/240 Vac, 60 Hz; or 2) 240 Vac, 50 Hz.

3.5.1.5 Image Array.

The camera shall have a solid state imaging array with a minimum effective picture element of 768 (H) x 494(V). The image array shall be free of blemishes as defined by EIA-330.

3.5.1.6 Resolution.

The camera shall provide not less than 380 lines of horizontal resolution. The resolution shall not vary over the life of the camera.

3.5.1.7 Sensitivity.

The camera shall be capable of providing full video output using a F/1.4 lens, 1/60 second shutter, and scene illumination of 1.7 lux.

3.5.1.8 Connectors.

The camera connectors shall interface with other CCTV system components and be compatible with the ICIDS communication links in use.

3.5.1.9 Automatic Circuits.

The camera shall have automatic black level, automatic white clipper, and automatic gain control.

3.5.1.10 Camera Enclosures.

Any ancillary enclosure, with mounting hardware, needed to install the camera shall be provided as part of the enclosure. All enclosures must be capable of supporting Pan Tilt Zoom (PTZ).

> Note: Throughout this specification the words “housing” and “enclosure” are interchangeable.

3.5.1.10.1 Indoor Camera Enclosure.

The enclosure shall be a tamper resistant enclosure for indoor camera operation. It shall be equipped with tamper resistant latches, and shall be supplied with the proper mounting brackets for the specified camera and lens.

3.5.1.10.2 Outdoor Camera Enclosure.

The outdoor camera enclosure shall be used to provide a condensation free environment for camera operation under exterior conditions. The enclosure shall be equipped with any supplemental camera mounting blocks needed to position the camera and lens to maintain the proper optical centerline. All electrical and signal connections required for operation of the camera shall be provided on the rear of the enclosure. A mounting bracket, which can be adjusted to center the weight of the enclosure and camera, shall be provided as part of the enclosure.

3.5.1.11 Lenses.

Camera lenses shall be provided with the camera and selected to provide coverage of the required field of view. The camera and lens shall be equipped with an auto-iris mechanism. Lenses shall not be used on a camera with an image format larger than the lens is designed to cover.

3.5.1.12 Video Monitors.

The monitors shall display color and conform to UL-1410 specifications.

3.5.1.12.1 Power.

The monitors shall be capable of operating on supplied facility power. Nominal voltages and frequencies are: 1) 120/208/240 Vac, 60 Hz; or 2) 240 Vac, 50 Hz.

3.5.1.12.2 Display Size.

The monitor shall have a display size of 15 inches or greater, measured diagonally.

3.5.1.12.3 Controls.

Controls used during normal operations shall be accessible from the front panel.

3.5.1.12.4 Monitor Mounting.

Site specific conditions and user operating standards require that monitor enclosures and mounting configurations be flexible. Monitors may be mounted in an EIA standard rack or use wall or ceiling mounting.

3.5.1.13 Stored Video Monitor.

The CCTV system shall provide an additional monitor for assessment of stored video. This monitor may also be manually selected and used for alarm assessment. This monitor shall be identical with the other CCTV monitors.

3.5.1.14 Video Switcher.

Electronic components, subassemblies, and circuits of the switcher shall be solid state. The switcher shall be a modular system that will allow for expansion or modification of inputs, outputs, alarm interfaces, and secondary control stations by addition of appropriate modules. Switcher components shall be capable of operating on either of the following nominal voltages and frequencies depending on available facility power: 120/208/240 Vac 60 Hz or 240 Vac 50 Hz switchable either manually or automatically. All components, modules, cables, power supplies, software, and other items needed for a complete and operable CCTV switching system shall be provided.

3.5.1.14.1 Software.

If the video switcher is software programmable, the software shall be supplied as part of the switcher. The software shall be installed in the switcher and shall be configured as required by the site design. Changes or alteration of features under software control shall be accomplished through on-site software programming. The switcher shall retain the current program and camera-monitor assignments in the event of power loss and shall not require reprogramming in order to restart the system.

3.5.1.14.2 Switcher Matrix.

The switcher shall be programmable, capable of switching any video input to any video output and have a switch matrix capacity of at least 128 video inputs. The video outputs shall be routed to the assessment monitors, as well as to the stored video monitor, as described. The video input capacity shall be expandable in increments of 64.

3.5.1.14.3 Alarm Interface.

The video switcher shall have an alarm interface compatible with the Primary Monitor Console (PMC) described in ICIDS-PS-0600. The CCTV assessment system shall accept commands from the PMC to display remote area camera video on up to four monitors of an automatic console selected or manually selected remote area. The interface shall have an automatic call-up feature whereby the receipt of an alarm from a remote area shall cause the video from that remote area to be displayed in near real time on the monitors. The monitors shall be blanked unless video is manually commanded or auto commanded.

3.5.1.14.4 Control Keyboards.

Any required control and programming keyboard(s) for the video switcher shall be supplied at the ICIDS security monitoring station. The control keyboard shall provide the interface between the operator and the CCTV system and shall relay commands to the switcher. It shall provide control of the video switcher functions needed for operation and programming the switcher. A program keyboard, if required, shall include, but not be limited to providing the following functions: programming the switcher, annotation programming, and manual video call-up. If the switcher requires an additional keyboard for system management functions, it shall be supplied with the switcher.

3.5.1.14.5 Accessory Control Equipment.

The video switcher shall be equipped with signal distribution units, pre-positioning cards, expansion units, cables, software or any other equipment needed to ensure the CCTV system is complete and fully operational.

3.5.1.15 Video Signal Equipment.

Electrically powered video signal equipment shall be capable of operating on either of the following nominal voltages and frequencies depending on available facility power: 120/208/240 Vac 60 Hz or 240 Vac 50 Hz switchable either manually or automatically. The equipment shall be furnished with power supplies and mounting equipment, as needed.

3.5.1.15.1 Ground Loop Correctors.

Ground loop correctors shall eliminate the measured ground loop interference in hard wire video transmission lines. They shall pass the full transmitted video bandwidth with no signal attenuation or loss. Ground loop corrector types include Clamps, Isolation Transformers, Isolation Amplifiers, and Differential Correctors.

3.5.1.15.2 Video Loss/Presence Detector.

The video loss/presence detector shall monitor video transmission lines for the presence of the video signal. The

detector shall annunciate an alarm when the video signal drops below a pre-set threshold level. The threshold level shall be adjustable for each video channel via a front panel control and reset. The video loss alarm shall be annunciated at the status display. The alarm indication shall be maintained until proper video has been established.

3.5.1.15.3 Video Equalizing Amplifier.

The video equalizing amplifier shall be designed to correct loss in video signal level and high frequency attenuation, if caused by long distance video signal transmission over hard wire systems. The amplifier shall have independent signal gain and equalization controls. The amplifier shall be capable of equalizing at least 900 meters of RG-11/U flexible coaxial armored or unarmored cable. The amplifier shall provide a minimum of 6 dB of video gain and 12 dB of high frequency compensation. Bandwidth shall be 10 MHz or greater and frequency response to 8 MHz shall be plus or minus 1 dB or less. Hum and noise shall be 50 dB below 1 volt peak-to-peak or better. Video inputs shall be 75 ohm, unbalanced, terminating differential grounded. Video outputs shall be 75 ohm, differential, source terminated, 1 volt peak-to-peak. Output isolation shall be 40 dB or greater at 5 MHz.

3.5.1.15.4 Video Distribution Amplifier.

The video distribution amplifier shall be designed to distribute a single, 75 ohm; unbalanced video signal to a minimum of four, 75 ohm, source terminated video outputs. It shall have not less than 3 dB of gain adjustment for the video outputs. Output isolation shall be 40 dB or greater at 5 MHz. Bandwidth shall be 10 MHz or greater and frequency response to 8 MHz shall be plus or minus 0.5 dB or less. Hum and noise shall be 55 dB below 1 volt peak-to-peak or better.

3.5.1.15.5 Video Annotation Equipment.

Video annotation equipment shall be provided. The annotation shall be alphanumeric and programmable for each video source. Annotation to be generated shall include, but not be limited to: individual video source identification, time (hour, minute and second) in a 24 hour format, date (year, month and day), and a unique user-defined title with at least 8 characters. The

annotation shall be inserted onto the source video so that both shall appear on a monitor or the digital video storage equipment. The lines of the annotation shall be movable for horizontal and vertical placement on the video picture. The annotation shall be automatically adjusted for time and date. Programmed annotation shall be retained in memory in the event of AC power loss.

3.5.1.15.6 Digital Video Storage and Playback Equipment.

3.5.1.15.6.1 Digital Video Recorder (DVR).

The DVR shall be specifically designed as a time lapse recorder for use in security systems. It shall be capable of operating on either of the following nominal voltages and frequencies depending on the available facility power: 120/208/240 Vac 60 Hz or 240 Vac 50 Hz. Resolution of the DVR, in normal play mode, shall not be less than 350 horizontal lines. Signal-to-noise ratio shall not be less than 40 dB. The DVR shall annunciate malfunction of the recorder to the operator. The recorder shall provide a connector for alarm trigger signal input.

3.5.1.15.6.2 Recording and Playback.

The DVR and/or its media shall be capable of storing 240 hours or more of video. It shall have at least 6 user selectable time-lapse record speeds. An alarm from the PMC shall automatically activate the recorder. The recorder shall begin recording in 1 second or less. The DVR shall put a cue mark or digital watermark on storage media at the beginning of an alarm event. The alarm event record time shall be selectable for up to 3 minutes of automatic recording as a minimum. These events will be flagged for easy access by reviewing authority. A record-lock feature shall be provided which will protect the DVR against tampering with the storage and power controls once recording has started. Playback functions shall include: alarm, fast forward search, fast reverse search, reverse/fast forward, play, slow motion or step field/frame, and pause/still.

3.5.1.16 Racks.

The monitor area components described in this Performance Specification shall be capable of being rack mounted. The rack(s) shall conform to EIA-310.

3.5.1.17 Enclosures.

Enclosures of all components shall conform to the Construction, All Television Equipment section and the Enclosures section of UL-1410.

3.5.1.18 Camera Support Equipment.

3.5.1.18.1 Interior Support Equipment.

For cameras mounted in interior locations, with or without interior enclosures, the camera shall be wall or ceiling mounted. The camera mount shall have an adjustable head for mounting the camera and be of sufficient length to allow for free and full adjustment of the camera.

3.5.1.18.2 Exterior Support Equipment.

The camera and lens contained in an environmentally sealed enclosure shall be installed on a camera support as defined in the subparagraphs below. Any ancillary mounting hardware needed to install the support and install the camera on the support shall be provided as part of the support. All exterior support systems shall provide easy access for camera installation and maintenance.

3.5.1.18.2.1 Cantilever Camera Support.

The camera mounting pole shall be a straight or hinged, cantilever corrosion resistant pole with counterweights and mounting base. All fittings shall be of corrosion resistant material. The pole shall be capable of supporting the camera and enclosure and shall be rated for a wind load of 161 km per hour. The camera mounting plate shall locate the camera 4.6 meters vertically from the base and 2.7 meters horizontally from the centerline of the pole to the centerline of the camera. The pole shall have an internal wiring harness that routes the video, sync and power between the pole base and camera mount. The wiring harness shall be compatible with the camera to be mounted on the pole. Surge protection shall be provided at the pole between the wiring harness and the incoming electronic signal lines and power line. The pole shall have a weatherproof AC power service outlet that is surge protected and has a ground

fault interruption device. Separate circuit breakers shall be provided for camera power and service outlet AC power.

3.5.1.18.2.2 Straight Camera Pole.

The camera mounting pole shall be either a straight corrosion resistant pole or a hinged and counterweighted straight corrosion resistant pole and mounting base. All fittings shall be of corrosion resistant material. The pole shall be capable of supporting the camera and enclosure and shall be rated for a wind load of 161 km per hour. The camera mounting plate shall locate the camera 4.7 m vertically from the base and 0.5 m horizontally from the centerline of the pole to the centerline of the camera. The pole shall have an internal wiring harness that routes the video, sync and power between the pole base and camera mount. The wiring harness shall be compatible with the camera to be mounted on the pole. Surge protection shall be provided at the pole between the wiring harness and the incoming electronic signal lines and power line. The pole shall have a weatherproof AC power service outlet that is surge protected and has a ground fault interruption device. Separate circuit breakers shall be provided for camera power and service outlet AC power.

3.5.1.18.2.3 Wall Mount.

The camera mount shall have an adjustable head for mounting the camera and be of sufficient length to allow for free and full adjustment of the camera. The wall mount and head shall be capable of supporting the camera and enclosure. The wall mount and head shall be constructed of corrosion resistant materials.

3.5.2 Interchangeability.

The CCTV assessment equipment shall:

a. Be interchangeable with any like equipment.
b. Not have soldered connections between any replaceable subassemblies.

3.6 Human Factors Engineering (HFE).

Paragraph 3.8 of ICIDS-PS-0600 shall apply.

3.7 Safety.

The CCTV shall not expose operators, administrators, or maintenance personnel to electrical or mechanical hazards.

3.8 Environmental Requirements.

3.8.1 Natural Environment.

The components of the CCTV shall withstand environmental conditions, or combinations thereof, as follows:

3.8.1.1 Interior Components.

3.8.1.1.1 Non-Operating Conditions.

There shall not be any damage in any temperature between -30C and +60C.

3.8.1.1.2 Operating Conditions.

a. Temperature. The CCTV components shall be able to operate, as specified herein, in any temperature between +10C and +40C.

b. Relative Humidity. The CCTV components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

3.8.1.2 Exterior Components.

3.8.1.2.1 Non-Operating Conditions.

There shall not be any damage in any temperature between -40C and +60C.

3.8.1.2.2 Operating Conditions.

a. Temperature. The CCTV components shall be able to operate, as specified herein, in any temperature between -10C and +50C.

b. Relative Humidity. The CCTV components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

c. Rain. The CCTV exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 57.

d. Dust. The CCTV exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 58.

3.8.2 Impact Conditions.

The CCTV components shall not be damaged and shall operate, as specified herein, when subjected to the jarring test, as specified in UL 1076 Section 39.

3.8.3 Vibration Conditions.

The CCTV shall not be damaged by vibration when tested as specified in UL 639, Section 37.

3.9 Electromagnetic Compatibility.

3.9.1 Electromagnetic Radiation.

The CCTV components shall comply with the requirements of Federal Communication Commission (FCC) Standard Part 15, Class B equipment.

3.9.2 Induced Environment.

The CCTV components shall meet lightning and EMI transient requirements of UL 1076, Section 44 and 45.

3.9.3 Surge Protection.

3.9.3.1 Power Lines.

All equipment connected to AC power shall be surge protected. Equipment protection shall meet the requirements of ANSI C62.41. Fuses shall not be used for protection.

3.9.3.2 Video and Sync Signal Transmission Lines.

All electrical cables used for sync and video transmission shall include protective devices to safeguard the CCTV equipment against surges. The surge suppression devices shall not attenuate the video or sync signal under normal conditions. Fuses shall not be used for surge protection.

3.10 Finish.

3.10.1 Treatment and Painting.

Unless otherwise specified, the portions of the components subject to corrosion shall be cleaned, treated and painted.

3.11 Identification Plate or P/N Marking.

All components of the CCTV shall be identified with make, model/part number and serial number in accordance with UL 1076.

3.12 Workmanship.

The workmanship shall be in accordance with best commercial standards and practices as specified in UL 1076. These requirements are applicable to wiring, welding, brazing, plating, riveting, finishes, machine operations, screw assemblies, and freedom of parts from burrs, sharp edges, or any other damage or defect that could make the part (or equipment) unsuitable for the purpose intended.

4. VERIFICATION.

Verification is the process of inspection to show that the CCTV system, while functioning within the ICIDS, meets the requirements of this specification. All inspection results shall be documented in contractor prepared reports. The Government reserves the right to perform any of the inspections set forth in this specification, where such inspections are deemed necessary to ensure supplies and services conform to the prescribed requirements. The inspection requirements, specified herein, are classified as follows:

a. Performance Verification Test (PVT-1) (see 4.2.1).

b. Performance Verification Test (PVT-2)/System Performance Verification (SPV) (see 4.2.2).

4.1 Methods of Verification.

Table 1 provides the methods utilized to accomplish verification including:

a. Contractor performed analysis (C/A)is an element of verification that utilizes established technical or mathematical models or simulations, algorithms, charts, graphs, circuit diagrams, or other scientific principles or procedures to provide evidence that the stated requirements were met. An "x" in the C/A column of Table 1 indicates that details of the analysis performed by the Contractor shall be provided in the Test Plan and the analysis shall be included in the Test Report.

b. Contractor performed examination (C/E) is an element of verification and inspection consisting of investigation, without the use of special laboratory appliances or procedures, of items to determine conformance to specified requirements. Examination is generally nondestructive and typically includes the use of simple physical manipulation, mechanical and electrical gauging and measurement. An "x" in the C/E column of Table 1 indicates that the Contractor conducted examination shall be included in the Test Plan, and the results of the examination shall be included in the Test Report.

c. Contractor performed test (C/T) is an element of verification and inspection which generally denotes the determination, by technical means, of the properties or elements of items, including functional operation, and involves the application of established scientific principles and procedures. An "x" in the C/T Column of Table 1 indicates that the Contractor conducted

test shall be included in the Test Plan. Details shall be provided in the Test Procedure, and the results of the tests shall be included in the Test Report.

4.2 Performance Verification Inspection.

Performance verification inspection includes:

4.2.1 Performance Verification Inspection – 1

Performance Verification Inspection – 1 includes analysis, examination, and PVT-1 of the fully integrated ICIDS-IV system consisting of at least one component of each hardware/software item. The Contractor shall conduct the test, in accordance with (IAW) Government approved test plans and procedures and using the test methods described in Table 1, to verify the ICIDS system performance.

4.2.2 Installed Performance Verification Inspection – 2

Performance Verification Inspection – 2 includes analysis, examination, and PVT-2 of the first installed ICIDS-IV system to verify performance prior to Government acceptance. Contractor generated, Government approved test plans and test procedures shall be utilized using the test methods described in Table 1 to verify acceptable system performance.

4.2.3 Installed System Acceptance Inspection

Installed System Acceptance Inspection includes analysis, examination, and System Acceptance Test (SAT) of each installed ICIDS-IV system, subsequent to the first system, to verify performance prior to Government acceptance. Contractor generated, Government approved test plans and procedures shall be utilized using the test methods described in Table 1 to verify acceptable system performance.

TABLE 1

Paragraph	C/A	C/E	C/T
3.5.1 Camera		x	

Paragraph	C/A	C/E	C/T
3.5.1.1 Signal-to-noise-ratio	x		
3.5.1.2 Distortion	x		
3.5.1.3 Lens mount.		x	
3.5.1.4 Power.			x
3.5.1.5 Image array	x		
3.5.1.6 resolution	x		
3.5.1.7 Sensitivity	x		
3.5.1.9 Connectors		x	
3.5.1.10 Automatic circuits			x
3.5.1.11 Camera enclosures		x	
3.5.1.11.1 Indoor Camera Enclosure		x	
3.5.1.11.2 Outdoor Camera Enclosure		x	
3.5.1.12 Lens	x		
3.5.1.13 - 3.5.1.14 Video monitor			x
3.5.1.15 - 3.5.1.15.6 Video switcher			x
3.5.1.16 - 3.5.3.16.6.2 Video signal equipment			x
3.5.1.17 – 3.5.1.19 Mounting and Enclosures		x	
3.5.7 Interchangeability.		x	
3.6 HFE.		x	
3.7 Safety.		x	
3.10 Finish.		x	
3.11 ID Plate or P/N Marking.		x	
3.12 Workmanship.		x	

5. Definitions.

Definitions of terms as used in this specification.

5.1 Damage.

Damage is defined as deformation, corrosion, loosening of parts, breakage, change of fit of any part, physical change which impairs the mechanical integrity of the component, evidence of delamination or water penetration into integrated circuits, printed circuit boards or parts resulting in non-conformance of a component to the provisions of this performance specification.

DRAFT

31 OCTOBER 2005
Revision 0
ICIDS-PS-0602

PERFORMANCE SPECIFICATION

FOR

ENTRY CONTROL EQUIPMENT

OF THE

INTEGRATED COMMERCIAL INTRUSION

DETECTION SYSTEM IV

DRAFT V3

TABLE OF CONTENTS

1. **SCOPE.**

1.1 Identification.

This Performance Specification (PS) covers the Entry Control Equipment (ECE) subsystem of the Integrated Commercial Intrusion Detection System (ICIDS).

1.2 Subsystem Description

The ECE subsystem functions as a part of the ICIDS to control individual access to restricted areas. The ECE will deny entry to any individual attempting to enter without the proper credentials. Denied entry alarms are reported to the ICIDS central monitoring location for assessment and response. The subsystem will be capable of interfacing with any standard credential, including but not limited to, the DOD Common Access Card (CAC), commercial “Smart” Cards, and those cards and devices utilizing biometric identifiers. The subsystem shall have the capability to store all access transactions for future retrieval.

1.3 Subsystem Overview

There are two (2) applications of the ECE subsystem.

1) Exterior secure areas.
2) Interior secure areas.

Unless otherwise specified, the requirements pertain to all applications.

2. **APPLICABLE DOCUMENTS**

The following documents of the issue in effect on the date of request for proposal form a part of this description to the extent specified herein.

2.1 Government Documents.

ICIDS-PS-0600	Performance Specification (PS) for Command, Control, and Display Subsystem of the Integrated Commercial Intrusion Detection System

SEIWG-012	28 February 1994	Prime Item Product Function Specification for Magnetic Stripe Credentials (MSC)

2.2 Non-Government Documents.

2.2.1 Underwriters Laboratories (UL) Standards.

UL 294	29 January 1999	Access Control System Units.
UL 639	21 February 1997	Intrusion-Detection Units.
UL 1076	29 September 1995	Proprietary Burglar Alarm Units and Systems.

(Application for copies should be addressed to the Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062.)

3. **REQUIREMENTS.**

3.1 Description.

The ECE specified herein is to be used in conjunction with the ICIDS, as defined in ICIDS-PS-0600, to control entry and exit to secure areas and to alert security monitors of attempts at unauthorized entry. The ECE configuration described herein is intended to illustrate functional requirements only and is not intended as a design constraint. Entry control devices installed in a remote secure area are directed by a local controller. The local controllers interface, via the Remote Area Data Collectors (RADCs) and the CCDS, to the network controller/enrollment terminal. The size of this network is determined by the number of secure areas requiring entry control. The security level of each local area is utilized to determine if ECE is required and the type of access credential required.

3.1.2 Major Components:

a. Network Controller/Enrollment Terminal,
b. Printer,
c. Network Controller Backup Power Supply,

d. Local Controller,
e. Local Controller Backup Power Supply,
f. Key Pad,
g. Card Reader,
h. Biometric Input Device,
i. Combination Key Pad/Card Reader,
j. Card Reader Card,
k. Electric Door Locks (Types 1 through 4),
l. Exit Push Button,
m. Entry Control Equipment/Remote Area Data Collector (RADC) Interface,
n. Badging Station.

Note: Not all sites will require all major components.

3.1.3 UL Listing.

ECE components shall be either UL listed or meet the requirements of UL 294.

3.2 Reliability.

The network controller/enrollment terminal and local controller shall each have a minimum Mean-Time-Between-Failure (MTBF) of 82,000 hours. The entry/exit control devices (key pad, card reader, biometric input device, combination key pad/card reader) shall each have a minimum MTBF of 216,000 hours. The electric door lock, exit push button, and door lock sensor switch shall each have a minimum Mean-Activations-Between-Failure (MABF) of 18,000 activations.

3.3 Construction.

Section 3.2 of ICIDS-PS-0600 shall apply.

3.4 Maintainability.

Section 3.3 of ICIDS-PS-0600 shall apply.

3.4.1 Maintenance Ratio.

Maintenance ratio is defined as the ratio of the total active maintenance man-hours required (scheduled and unscheduled) to the total operating time. Man-hours for repair of replaced components and scheduled before-and-after operation checks are excluded. The maintenance ratio for both the network controller/enrollment terminal and local controller shall not exceed 0.000006. The maintenance ratio for entry/exit control devices (keypad, card reader, biometric input device,

combination keypad/card reader) shall not exceed 0.000002. A maintenance schedule shall be established prior to the start of any testing.

3.4.2 Preventive Maintenance.

Section 3.3.4 of ICIDS-PS-0600 shall apply.

3.5 Performance Characteristics.

3.5.1 General System Functions.

When the entry control equipment is installed and operational with the ICIDS console, it shall function as a combined system. The system shall:

a. verify the validity of requests for access and either permit or deny access,

b. notify the requester of acceptance or denial,

c. output the proper control signal to open the access point, lock after access is completed, and provide a door unlocked alarm if the door does not close and lock within the specified time,

d. allow the requester a preprogrammed number of additional requests for access if access is denied on the first request. An access-denied signal shall be output at the entry control device (e.g., red LED at the key pad), at the network controller (e.g., printer and display message), and at the operator console if additional requests for access are denied,

e. allow a duress alarm to be output by the entering of a special code into a key pad or by activating a panic switch. Display the duress alarm at the network controller and operator console, but provide no indication of duress alarm at the local controller or key pad,

f. have a minimum throughput of 6 authorized entries per minute.

3.5.1.1 Major Component Functions.

3.5.1.1.1 Network Controller/Enrollment Terminal.

The network controller/enrollment terminal shall be a programmable device which serves as the ECE network central processor, functions as an enrollment terminal, manages the enrollment database, provides enrollment data to the connected local controllers, and provides an interface either to create a badge or exchange the enrollment data with existing badging systems. The major components of the network controller/enrollment terminal are a display, alphanumeric keyboard, CPU, non-volatile memory, printer, removable storage media, local controller communication port(s), and back-up power supply.

3.5.1.1.2 Network Controller/Enrollment Terminal Functions.

The network controller/enrollment terminal shall:

a. provide enrollment capability. The network controller/enrollment terminal shall provide the hardware and software necessary to enroll and delete users from the system and create badges as needed. As a minimum, enrollment shall specify and allow control of a specific user's access to specified areas, at specified dates and times,

b. provide the following database management functions as a minimum: create a user file or record, append new users to the database, modify data for existing users, and backup all or user selected portions of the enrollment database to removable storage media. The database shall be capable of supporting at least 10,000 individual users having a card, a Personal Identification Number (PIN), a photograph, biometric data, personnel information, other credential, and combinations of credentials. The database shall contain, as a minimum for each enrolled user, the user's name, employee identification, card identification, and PIN. Data specifying identification of personnel shall be protected by passwords level of access,

c. provide a non-volatile storage device for the system software and enrollment database. The system shall have the capability to automatically reinitialize when power is restored after an equipment failure or power

outage without loss of the database or necessary operating data,

d. provide for at least four levels of operator access to the functions of the network controller/enrollment terminal. The capability shall be provided to assign the system functions to any of the four operator access levels. Operator access may be controlled by password, card, PIN, or other positive means of identification,

e. provide automatic non-volatile storage of at least the 50,000 most recent events (e.g., entry approvals, entry denials, duress alarms, etc.). When this historical log becomes full, new events shall replace the oldest events in a first-in-first-out fashion. The system shall provide the capability to erase, print, and backup all or part of the historical log to make space available for new events. A warning message shall be displayed to the operator when the historical log is nearly full,

f. display all system alarms (e.g., duress, door unlocked, AC power loss, etc.). The display shall be visual, of a type adequate to allow, as a minimum, alphanumeric messages to be reported clearly to the operator,

g. provide a printer and associated software to automatically print events specified by the system maintainer in a format specified by the system maintainer as the events occur (e.g., automatic exception reporting). The printer software shall also provide the capability to generate reports in a format specified by the system maintainer which are keyed to any field of the database (e.g., all events between specified times, for specified users, at specified portals, etc.). Printing reports shall be accomplished on-line and not interfere with normal system operation,

h. provide for control and communications to a minimum of 64 local controllers (expandable in modular increments to full system capacity). The network controller shall be capable of communicating with local controllers separated by a distance of up to sixteen

kilometers without repeaters. The sixteen kilometer minimum communication distance shall apply to any communication architecture (i.e., multidrop loop, star (individual), etc.). The use of fiber optics in lieu of hardwired lines is permissible,

i. automatically downloads the appropriate initial database information and appropriate database changes to each local controller to which the specific enrollment information applies,

j. incorporate built-in diagnostics implemented in software/firmware, hardware, or both. Each time the processor is powered it shall automatically execute a series of built-in tests and report equipment malfunctions, configuration errors, and inaccuracies to the printer or display. Diagnostic aids shall be provided within the network processor to aid in set-up, maintenance, and troubleshooting.

3.5.1.1.3 Network Controller/Enrollment Terminal Backup Power Supply.

An Uninterruptible Power Supply (UPS) shall be available, which shall meet the requirements stated in paragraph 3.4.2.1.10 of ICIDS-PS-0600.

3.5.1.1.4 Local Controller.

The local controller shall be capable of complete stand-alone entry control operation after enrollment information is downloaded from the network controller/enrollment terminal.

The local controller also shall:

a. be capable of controlling access (entry and exit) to a minimum of two doors and shall be capable of incremental increases to eight doors,

b. interface to up to eight electric door locks with or without door lock sensors, and sixteen entry/exit devices (i.e., key pads, card readers, biometric devices, or combinations thereof). Note: The sixteen entry/exit devices are divided into eight entry devices and eight exit devices corresponding to the eight doors,

c. be capable of controlling access of not less than 10,000 users, each identified by individually unique cards, PINs, biometric identifiers, or combinations thereof,

d. deny any card, PIN, biometric identifiers, or combination thereof, not authorized for that particular controller,

e. be capable of providing at least four security levels to which each user can be assigned. Any attempt to access an area beyond any individual's pre-defined security level shall result in an access denial alarm after the preprogrammed number of attempts,

f. restrict the time between the access request and allowed access to less than 3 seconds or a longer time, up to 10 seconds, as approved by cognizant authority and selected by the system maintainer. The door lock shall be open to allow access for no longer than the time entered by the system maintainer. A door unlocked alarm shall be transmitted to both the network controller and RADC if any door remains open or otherwise unlocked longer than the 3 second entry time or longer than the entry or exit time selected by the system maintainer,

g. provide the capability for the incorporation of anti-passback functions. Once an authorized individual has passed through a portal, the system shall not allow use of the same identifier to allow entry through any portal of the same security level or lower until the individual has left the area through any portal of the same security level. Any attempt to violate the anti-passback procedures shall result in an entry denial alarm,

h. have an internal battery to prevent loss of volatile memory in the case of power failure,

i. incorporate continuous line supervision of at least communications and power status,

j. provide the database management functions necessary for the local controller database,

k. provide a memory buffer which shall be updated as required to contain the most recent 128 events (minimum) in a first-in-first-out fashion. In the event of a communication loss or interruption, the local controller shall upload this buffer to the network controller once communication is restored,

l. provide communications to the network controller, or other local controllers depending on system architecture. The local controller shall be capable of communicating to the network controller, either directly or via other local controllers, separated by a distance of up to sixteen kilometers without repeaters. The sixteen kilometer minimum communication distance shall apply to any communication architecture (i.e., multidrop loop to other local controllers, star (individual) directly to the network controller, etc.). The local controller shall communicate all events (access approved, denied, tamper, duress, etc.) to the network controller as they occur. The communication links shall be such that the use of fiber optics is permissible,

m. provide key pad and card reader line supervision. Line supervision shall be provided whether the key pad is interfaced directly to the local controller or to the card reader such that any opening or shorting shall result in a tamper alarm transmitted to the network controller and to the RADC,

n. be provided with a tamper switch(s) for each enclosure housing) opening, local controller, key pad, or card reader. Opening or attempted removal of an enclosure (housing), or enclosure (housing) cover will result in declaration of a tamper alarm.

3.5.1.1.5 Local Controller Backup Power Supply.

Backup power supply shall meet the following requirements:

a. Operate on either of the following nominal voltages and frequencies, depending on available facility power:

(1) 120/208/240 Vac, 60 Hz.
(2) 220 Vac, 50 Hz.

b. Include battery backup capable of supplying sufficient power to the local controller during facility power interruptions, for a minimum of 8 hours, at the lowest specified temperature,

c. The battery shall be sufficiently recharged, within 12 hours after the return of primary power, to provide power through another minimum 8 hour primary power interruption,

d. Continuously monitor the battery voltage. If an over-voltage condition is measured at the battery terminals, the primary AC supply and battery charging circuit shall be disabled and operation shall continue on the battery. If an under-voltage condition is measured at the battery terminals while operating from the battery, the positive battery lead shall be disconnected to prevent excessive discharge. The battery lead shall be automatically reapplied after return of primary AC power. If a DC supply output out-of-tolerance condition is measured, indicating a power supply failure, both the primary AC and battery shall be disabled. Any power loss shall be reported to the PMC,

e. Be capable of sustaining momentary overloads of 125% of rated capacity for up to 10 minutes, and sustaining surges of 150% of rated capacity for 10 seconds,

f. Include EMI, transient, and surge protection in accordance with ICIDS-PS-600, paragraph 3.11, to prevent damage to equipment from lightning and other conducted electrical disturbance, or to localize damage to easily repairable, low-cost components.

3.5.1.1.6 Key Pad.

The key pad may be used alone or in conjunction with a card reader to control access or exit through a locked door by means of a unique combination of alphanumeric keys entered by a user.

3.5.1.1.6.1 Key Pad Functions.

As a minimum, the key pad shall:

a. provide a minimum of ten alphanumeric character keys,

b. read the sequence of keys entered by the user, the user's (PIN), and communicate the sequence to the local controller,

c. provide no restriction to the length of the key sequence (PIN) up to a limit of ten characters (i.e., the length of the PIN may be variable for each installation site),

d. provide an indication of entry/exit authorized or unauthorized (e.g., red LED for entry denied, green LED for entry approved) in response to a signal from the local controller.

3.5.1.1.6.2 Key Pad Power.

Key pad power may be supplied by the local controller, card reader, or other source as necessary.

3.5.1.1.6.3 Key Pad Physical Characteristics.

The key pad, if used as the sole entry controller, shall be provided in its own enclosure, suitable for flush and surface mounting. If used in conjunction with a card reader, the key pad may be in the same enclosure with the reader. In either case, the enclosure shall be tamper protected.

3.5.1.1.7 Card Reader.

The card reader shall operate using any one or more of the state-of-the-art devices of any technology (e.g., Wiegand effect, proximity technology, magnetic stripe [per SEIWG-012], CAC, “Smart” card, biometric).

3.5.1.1.7.1 Card Reader Major Functions.

As a minimum, the card reader shall:

a. read encoded cards and communicate the card information to the local controller,

b. provide an indication of entry/exit authorized or unauthorized (e.g., red LED for entry denied, green

LED for entry approved) in response to a signal from the local controller.

3.5.1.1.7.2 Card Reader Power.

Card reader power may be supplied by the local controller or other source, as necessary.

3.5.1.1.7.3 Card Reader Physical Characteristics.

The card reader, if not used in conjunction with a key pad, shall be provided in its own enclosure, suitable for flush and surface mounting. If used in conjunction with a key pad, the card reader may be in the same enclosure with the key pad. In either case, the enclosure shall be tamper protected.

3.5.1.1.8 Biometric Input Device.

The biometric input device may be used alone or in conjunction with a card reader or other devices, as necessary, to control access to a secure area by means of a set of biometric identifiers. It operates by sensing the physical characteristics presented (finger tip, palm, etc.) and converting them to digital parameters used for identification.

3.5.1.1.8.1 Biometric Input Device Major Functions.

As a minimum, the biometric input device shall:

a. sense the physical characteristics presented (finger print, hand geometry, iris, etc.), convert them to the digital parameters used for identification, and communicate the parameters to the identification database,

b. provide an indication of entry/exit authorized or unauthorized (e.g., red LED for entry denied, green LED for entry approved), if operating as a stand alone device.

3.5.1.1.8.2 Biometric Input Device Power.

Biometric input device power may be supplied by the local controller or other source as necessary.

3.5.1.1.8.3 Biometric Input Device.

The biometric input device shall be provided in its own enclosure, suitable for flush and surface mounting. If used in conjunction with another device, the biometric input device may be in the same enclosure with the other device. In either case, the enclosure shall be tamper protected.

3.5.1.1.9 Combination Key Pad/Card Reader.

The combination key pad/card reader shall provide the combined functionality of the individual key pad and individual card reader specified in 3.7.1.1.6 and 3.7.1.1.7, respectively. Either, or both, may be utilized with the biometric input device specified in 3.7.1.1.8, as necessary.

3.5.1.1.10 Card Reader Cards.

Card reader cards shall:

a. be compatible with the card reader specified in 3.7.1.1.7 and 3.7.1.1.8 (e.g., Wiegand effect, proximity technology, magnetic stripe (IAW SEIWG-012), CAC, “Smart” card, biometric, etc.),

b. be not less than 5.08 cm by 7.62 cm or greater than 6.35 cm by 8.89 cm in size,

c. be resistant to forgery, tampering, alteration, and unauthorized extraction of data,

d. be provided with unique identifier codes. A minimum of 10,000 identifier codes shall be available,

e. be designed to last not less than 2 years.

3.5.1.1.11 Electric Door Locks.

Electrical door locks shall be of the electrical release type and shall interface to the local controller and be fully compatible with the rest of the entry control equipment of this Performance Specification. They shall be reversible for use on left-hinged and right-hinged doors. The electric door locks shall be provided with sensors to detect if the locking mechanism is locked or unlocked. These sensors shall be so designed that they detect the actual condition of the locking mechanism. The electric door locks shall be available both with and without the sensors.

3.5.1.1.12 Electric Door Lock Power.

The electric door locks may be powered from the local controller, key pad, card reader, combination key pad/card reader, or other source as necessary.

3.5.1.1.13 Master Key.

All electric door locks shall have a provision for manual mechanical override using a master key.

3.5.1.1.14 Exit Push Button.

An exit push button shall be available for installation in the protected area by a door controlled by entry control equipment when anti-passback procedures are not required. The exit button, when pressed, shall release the electrical door lock for a preset time adjustable for between 2 and 10 seconds.

3.5.1.1.15 Emergency Egress.

An emergency egress capability shall be available to release the door lock and provide an alarm to the network controller of an emergency override.

3.5.2 Interface.

3.5.2.1 Key Pad Interface.

The key pad shall interface with the local controller either directly or via a card reader when used in conjunction with a card reader. The interface shall communicate the user's PIN to the local controller and shall communicate the entry/exit authorized/unauthorized signal from the local controller.

3.5.2.2 Card Reader Interface.

The card reader shall interface with the local controller. The interface shall communicate the user's card information and key pad PIN, when used in conjunction with the key pad, to the local controller and shall communicate the entry/exit authorized/unauthorized signal from the local controller.

3.5.2.3 Biometric Input Interface.

The biometric input device shall interface with the local controller either directly, when operating in a stand alone mode, or through a card reader or other device as necessary.

The local controller shall communicate the entry/exit authorized/denied signal for display.

3.5.2.4 ECE System/RADC Interface.

Section 3.4.2.2.8 of ICIDS-PS-0600 shall apply with the following additions.

3.5.2.4.1 Physical Interface.

The field wiring and internal wiring shall meet the conditions specified in UL 294, sections 10 through 17.

3.5.2.4.2 Electrical Interface Outputs.

All output signals shall last for 350 ± 100 milliseconds. The outputs shall have form "C" contacts rated at 0.25 A at 24 Vdc.

3.5.2.5 Enrollment/Badging Station.

Station shall include:

a. RSM Workstation with computer, keyboard and mouse or trackball device
b. Color Monitor
c. PC Camera
d. ID Card/Token Printer
e. Report/Logging Printer
f. Uninterruptible Power Supply (UPS)

3.5.3 Enclosures.

3.5.3.1 Construction.

All enclosures of entry control equipment shall meet UL 294, section 7.

3.5.4 Detection/False-Alarm Performance.

3.5.4.1 Access-Authorized Error Rate.

The rate at which the entry control equipment, when configured in its maximum configuration, denies access to an authorized, enrolled individual shall be less than 1.0 percent.

3.5.4.2 Access-Denied Error Rate.

The rate at which the entry control equipment, when configured in its maximum configuration, allows access to an unauthorized individual shall be less than 0.01 percent.

3.6 Human Factors Engineering (HFE).

Section 3.8 of ICIDS-PS-0600 shall apply.

3.7 Safety.

Paragraph 3.9 of ICIDS-PS-0600 shall apply.

3.8 Environmental Requirements.

3.8.1 Natural Environment.

Section 3.10.1 of ICIDS-PS-0600 shall apply.

3.8.1.1 Interior Components.

3.8.1.1.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -30 C and +60 C.

3.8.1.1.2 Operating Conditions.

a) Temperature. The ECE components shall be able to operate, as specified herein, in any temperature between +10C and +40C.

b) Relative Humidity. The ECE components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

3.8.1.2 Exterior Components.

3.8.1.2.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -30C and +50C.

3.8.1.2.2 Operating Conditions.

a. Temperature. The ECE components shall be able to operate, as specified herein, in any temperature between -10C and +50C.

b. Relative Humidity. The ECE components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

c. Rain. The ECE exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 57.

d. Dust. The ECE exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour, as specified in UL 639, Section 58.

3.8.2 Impact Conditions.

The ECE components shall not be damaged and shall operate, as specified herein, when subjected to the jarring test as specified in UL 1076 Section 39.

3.8.3 Vibration Conditions.

The ECE Shall not be damaged by vibration when also tested as specified in UL 639, Section 37.

3.9 Electromagnetic Compatibility.

3.9.1 Electromagnetic Radiation.

The ECE components shall comply with the requirements of Federal Communication Commission (FCC) Standard Part 15, Class B equipment.

3.9.2 Induced Environment.

The ECE components shall meet lightning, EMI transient, and power surge requirements of UL 1076, Sections 44 and 45.

3.9.3 Lightning.

Equipment shall be protected to prevent equipment damage as a result of transients conducted into the equipment through power, communication, and/or control lines by natural phenomena, such as lightning, or to localize damage in easily repairable, low-cost components.

3.10 Finish.

3.10.1 Treatment and Painting.

Unless otherwise specified, the portions of the components subject to corrosion shall be cleaned, treated and painted.

3.11 Identification Plate or P/N Marking.

All components of the ECE shall be identified with make, model/part number and serial number in accordance with UL 1076.

3.12 Workmanship.

The workmanship shall be in accordance with best commercial standards and practices. These requirements are applicable to wiring, welding, brazing, plating, riveting, finishes, machine operations, screw assemblies, and freedom of parts from burrs, sharp edges, or any other damage or defect that could make the part (or equipment) unsuitable for the purpose intended.

4. VERIFICATION

Verification is the process of inspection to show that the ECE system, while functioning within the ICIDS, meets the requirements of this specification. All inspection results shall be documented in contractor prepared reports. The Government reserves the right to perform any of the inspections set forth in this specification, where such inspections are deemed necessary to ensure supplies and services conform to the prescribed requirements.

The verification requirements specified herein are classified as follows:

a. Performance Verification Test – 1 (PVT-1)

b. Performance Verification Test – 2 (PVT-2) / System Acceptance Test (SAT)

4.1 Methods of Verification.

Methods utilized to accomplish verification are as defined in Paragraph 4.1 of ICIDS-PS-0600, using Table 1 of this specification.

4.2 Performance Verification Test – 1 (PVT-1)

4.2.1 Performance Verification Inspection – 1

Performance Verification Inspection – 1 shall be as stated in ICIDS-PS-0600, paragraph 4.2.1, utilizing Table 1 of this specification.

4.2.2 Installed Performance Verification Inspection – 2

Installed Performance Verification Inspection – 2 shall be as stated in ICIDS-PS-0600, paragraph 4.2.2, utilizing

Table 1 of this specification.

4.2.3 Installed System Acceptance Inspection

Installed System Acceptance Inspection shall be as stated in ICIDS-PS-0600, paragraph 4.2.3, utilizing Table 1 of this specification.

4.3 Performance Verification Test – 2 (PVT-2) / System Acceptance Test (SAT)

The contractor shall perform an on site inspection, prior to Government acceptance, to assure that the ECE, while functioning within the ICIDS, is completely operational.

Table 1

Paragraph		C/A	C/E	C/T
3.5.1	General System Functions			x
3.5.1.1.1	Network/Enrollment Terminal		x	
3.5.1.1.2	Network/Enrollment Functions			x
3.5.1.1.3	Net/Enroll Backup Power			x
3.5.1.1.4	Local Controller		x	
3.5.1.1.5	Local Controller Backup Power			x
3.5.1.1.6.1	Keypad Functions			x
3.5.1.1.7.1	Card Reader Functions			x
3.5.1.1.8.1	Biometric input device Functions			x
3.5.1.1.9	Combined/Keypad/Card Reader			x
3.5.1.1.10	Card Reader Cards		x	
3.5.1.1.11	Electric Door Locks		x	
3.5.1.1.14	Exit Push Button			x
3.5.2.1	Keypad Interface			x
3.5.2.2	Card Reader Interface			x
3.5.2.3	Biometric Input Interface			x

Paragraph		C/A	C/E	C/T
3.5.2.4	ECE/RADC Interface			x
3.5.4 Performance	Detection/False Alarm	x		x
3.6	HFE.		x	
3.7	Safety.		x	
3.8.1.1.1	Non-operating conditions.	x		
3.8.1.1.2	Operating conditions.	x		
3.8.2	Impact.	x		
3.8.3	Vibration.	x		
3.9	EMI Control.	x		
3.9.1	EMI radiation.	x		
3.9.2	Induced environment.	x		
3.10	Finish.		x	
3.10.1	Treatment & painting.		x	
3.11	ID Plate or P/N Marking.		x	
3.12	Workmanship.		x	

5. PACKAGING

Packing requirements will be specified in Section D of the contract.

6. NOTES

6.1 Intended Use.

The ECE covered by this Performance Specification is intended to be a subsystem of the ICIDS which is for fixed, ground-based installation use.

6.2 Definitions.

Definitions of terms as used in this specification.

6.2.1 Damage.

Damage is defined as deformation, corrosion, loosening of parts, breakage, change of fit of any part, physical change which impairs the mechanical integrity of the component, evidence of delamination or water penetration into integrated circuits, printed circuit boards or parts resulting in non-conformance of a component to the provisions of this Performance Specification.

6.2.2 “Smart Card”

A “Smart Card” is defined as an identification credential that contains special information of an individual nature such as digital certificates, digital signatures, and/or biometric identifiers.

6.2.3 Biometric Identifier

A Biometric identifier is a set of biological characteristics that are unique to an individual and may be used to positively identify a person. Examples of biometric identifiers are fingerprints, facial characteristics, iris pattern, and hand geometry.

6.2.4 Biometric Input Device

The biometric input device is defined as the input device which senses the biometric parameters being used as an identifier. Examples are a fingerprint pad, an iris scanner, a hand geometry sensing plate, and other biometric sensors. The input sensor shall have processing circuits and associated electronics included within its enclosure and transmit sensor data to the database or local controller. It shall operate in conjunction with other devices such as a card reader or keypad and communicate with a remotely located database.

Department of Army

Office of Provost Marshal General Fielding Plan

Integrated Commercial Intrusion Detection System-IV (ICIDS-II)

NOTE: *** = Base Realignment & Closure Commission.**

FY08

1. Fort Monmouth, NJ	**AMC ***
2. Milan AAP, TN	**AMC**
3. Crane Army Depot, IN	**AMC**
4. Adelphi Labs, MD	**AMC**
5. Fort Eustis, VA	**TRADOC**
6. Radford AAP, VA	**AMC**
7. Tobyhanna Army Depot, PA	**AMC**
8. Sierra Army Depot, CA	**AMC**
9. Kwajalen Atoll, Marshall IS	**SMDC**
10. Lima Army Tank Plant, OH	**AMC**

FY09

11. Torii Station, JPN	**USARPAC**
12. Holston AAP, TN	**AMC**
13. Lone Star AAP, TX	**AMC ***
14. Ravenna AAP, OH	**AMC**
15. Rocky Mountain Arsenal, CO AMC	
16. Corpus Christi Army Depot, TX	**AMC**
17. Rock Island Arsenal, IL	**AMC**
18. Detroit Arsenal (ATP), MI	**AMC**
19. Iowa AAP, IA	**AMC**
20. Lake City AAP, MO	**AMC**

FY10

21. Twin Cities AAP, MN	**AMC**
22. Sunny Point, NC	**MTMC**
23. River Bank AAP, CA	**AMC ***
24. Kansas AAP, KS	**AMC ***
25. Fort Bragg, NC (ICIDS-I)	**FORSCOM**
26. Fort Polk, LA (ICIDS-I)	**FORSCOM**
27. Fort Rucker, AL (ICIDS-I)	**TRADOC**

28. Vicenza, IT (ICIDS-I)	**USAREUR**
29. Fort Sill, OK (ICIDS-I)	**TRADOC**
30. Fort Gordon, GA (ICIDS-I)	**TRADOC**

FY11

31. Fort Riley (ICIDS-1)	**NWRO**
32. Fort Cambell (ICIDS-1)	**SERO**
33. Fort Bliss, TX (ICIDS-II)	**TRADOC**
34. Fort Hood, TX (ICIDS-II)	**FORSCOM**
35. Fort Richardson, AK (ICIDS-II)	**USARPAC**
36. Fort Meyer, VA (ICIDS-II)	**MDW**
37. Fort McNair, DC (ICIDS-II)	**MDW**
38. Fort Lewis, WA (ICIDS-II)	**FORSCOM**

ATTACHMENT A

Requirements

For
Development and production

Of

Equipment Publications

1. SCOPE. This Attachment to the Statement of Work (SOW) prescribes contractor requirements for preparing equipment technical publications.

2. APPLICABLE DOCUMENTS

2.1. SPECIFICATIONS AND STANDARDS

MIL-STD-40051-2	Department of Defense Standard Practice: Preparation of Digital Technical Information for Page Based Technical Manuals
MIL-STD-38784 (Including Notices 1&2)	Department of Defense Standard Practice for Manuals, Technical: General Style and Format Requirements

NOTE: MIL-STD-40051-2 will govern technical content requirements only; MIL-STD-38784 will govern style and format requirements only.

2.2. DATA ITEM DESCRIPTION.

DI-MISC-80711A	Scientific and Technical Reports

3. REQUIREMENTS FOR TECHNICAL MANUALS

3.1. The contractor shall develop the following Technical Manual (TM):

TM 5-6350-XXX-12&P	Operator's and unit Maintenance Manual Including Repair Parts and Special Tools List for Integrated Commercial Intrusion Detection System-IV (ICIDS-IV)

This TM shall be in accordance with this Attachment (Paragraph 3.), the DD Form 1423 for DI-MISC-80711A, and the following Military Specifications:

a. MIL-STD-40051-2, Department of Defense Standard Practice: Preparation of Digital Technical Information for Page Based Technical Manuals (Exclusive of style and format requirements) tailored at Enclosure 1 of this attachment, entitled "Page Based TM Requirements Matrix for TM-5-6350-XXX-12&P".

b. MIL-STD-38784, Department of Defense Standard Practice for Manuals, Technical: General Style and Format Requirements.

3.2. SOURCE DATA.

3.2.1. EXISTING SOURCE DATA. In addition to other contractor developed source data, the following items will be used as source data.

TM 5-6350-275-10	Operator's Manual for the Integrated Commercial Intrusion Detection System (ICIDS-I)
TM 5-6350-275-24&P	Unit, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List For The Integrated Commercial Intrusion Detection System (ICIDS)

Operator's User Guide	For Integrated Commercial Intrusion Detection System ICIDS-II MDI Version 6.2.X
TM 5-6350-297-12&P	Operator's and unit Maintenance Manual Including Repair Parts and Special Tools List for Integrated Commercial Intrusion Detection System-III (ICIDS-III)

This data will be furnished by the Government at the Start-of-Work Meeting.

3.2.2. APPROVED EQUIPMENT CHANGES. The contractor shall incorporate coverage for all Government-approved changes/2028s made to the equipment, up to delivery of the final equipment under this contract. Information based on Engineering Change Proposals or equivalents approved for the convenience of the contractor shall be incorporated into the draft manuals by the contractor at no additional cost to the Government.

3.3. MEETINGS. The TM start-of-work meeting shall take place at the contractor's facility. The Contractor shall be prepared to discuss all TM requirements as shown in this Attachment (Paragraph 3.), the DD Form 1423, Data Item A030, for DI-MISC-80711A. In-process reviews shall take place when approximately 30% and 70% of the TM have been developed. The Government may request additional in-process reviews as required. The contractor shall be prepared to have one or more in-process reviews in the Washington D.C. area and two at the Contractor facility.

3.4. VALIDATION. The contractor shall validate the TM at the contractor's facilities or a Government facility. All functional features and data shall be validated as operational and correct. Contractor's validation records shall be available for Government inspection at any time. The Government reserves the right to witness the contractor validation.

3.5. VERIFICATION. The Government will verify the TM at a site to be determined after contract award by performing 100 percent of the operating and maintenance procedures using target audience personnel. A 100 percent desk review of those portions of the publication not subject to hands-on performance, e.g., table of contents, theory, index, etc., will be conducted. All functional features of the TM will also be verified. The contractor shall provide at verification sufficient copies of each publication to be verified; appropriate office or work space; a working copy of the equipment to be verified, including hardware and software; personnel necessary to document changes to the publications and resolve hardware and software issues; all tools and test equipment required, in accordance with the maintenance concept or MAC, to perform all procedures in each manual.

3.6. INCORPORATION OF COMMENTS. SFAE-CBD-GN-FPS is the Government publications acceptance activity for this contract. Any publications comments received by the contractor from other Government activities shall be forwarded to the above address for disposition. All comments received during and after the PVT-2 and Endurance Test, SOW paragraph 4.2.2.2. shall be included in the final delivery of the manual.

3.7. OZONE DEPLETION. Maintenance procedures shall not use any substance known to cause ozone depletion.

3.8. DELIVERY. For all technical manuals prepared under this contract, the contractor shall deliver digital files IAW DD Form 1423, Data Item A030, for DI-MISC-80711A. The Government will require additional deliveries of the digital files during the development of the manual. The contractor shall provide the digital files, as is, for in process reviews and as requested by the Government in addition to the deliveries as called out on the DD Form 1423.

3.9. The contractor shall grant the Government unlimited rights to any and all data and products under this SOW.

3.10. STYLE AND FORMAT.

a. TRIM SIZES: Trim size for the manual as follows:

TM 5-6350-XXX-12&P: Shall be appropriately formatted for a vertical (portrait) finished trim size of 8-1/2 inches by 11 inches.

b. FONTS: All manuals shall be prepared using the identical type styles used in the existing manuals (regular, bold, italics, bold italics) with symbols to match. All fonts in both the delivered Microsoft Word and Adobe Acrobat PDF files must be embedded.

c. All draft deliveries of the manual shall have the words “DRAFT–NOT FOR IMPLEMENTATION” printed across the top of the cover and every page of the manual.

d. ILLUSTRATIONS:

(1) Line Drawings. Line drawings, including exploded views, locator views, and detailed views, shall be used to support the operational and maintenance procedures and the RPSTLs. Photographs and engineering drawings will not be used.

(a) RPSTL Illustrations. The contractor shall prepare a separate figure for each breakdown of a repairable assembly. If an assembly is used more than once in a RPSTL, the Table of contents shall refer to the first appearance of the illustration with the following statement, "SEE GROUP XX FOR PARTS BREAKDOWN." Existing illustrations, government owned, or commercial illustrations, shall be used if they meet the requirements of MIL-STD-40051-2 and this SOW, otherwise the contractor shall prepare new illustrations. If an existing illustration requires more than 25 percent additions and/or deletions of callouts, the callouts of that illustration shall be completely re-sequenced. For reference-designated equipment, all electronic equipment and components to include cable assemblies shall be identified by the applicable reference designator on the illustration of that particular functional group.

(b) Multi-sheet RPSTL Figures. Multi-sheet figures may be used if appropriate, however, no more than three (3) sheets will be allowed within any RPSTL figure.

(2) Contractor’s illustration identification number may be used.

3.11. PACK-UP OF OPERATOR’S TMs WITH EQUIPMENT. The contractor shall pack the following with each equipment package delivered under this contract:

Two (2) paper copies of the TM
One (1) CD-ROM with Adobe Acrobat PDF files

ENCLOSURE 1

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
FRONT MATTER	R	R	R	R	5.2.1	<paper.frnt>
Front cover	R	R	R	R	5.2.1.1	<frntcover>
(MC) Promulgation letter					5.2.1.2	<promulgation>
Warning summary		R			5.2.1.3	<warnsum>
Change transmittal page					5.2.1.4	<chgsheet>
List of effective pages / work packages *(Excluding pocket TMs and publications with less than eight pages)*	R	R	R	R	5.2.1.5	<loepwp>
Title block page	R	R	R	R	5.2.1.6	<titleblk>
Table of contents	R	R	R	R	5.2.1.8	<contents>
How to use this manual	R	R	R	R	5.2.1.9	<howtouse>
CHAPTER 1. GENERAL INFORMATION, EQUIPMENT DESCRIPTION AND THEORY OF OPERATION	R	R	R	R	B.5.1	<gim>
GENERAL INFORMATION WORK PACKAGE	R	R	R	R	B.5.2	<ginfowp>
Scope	R	R	R	R	B.5.2.3	<scope>
Maintenance forms, records, and reports	R	R	R	R	B.5.2.4	<mfrr>
Reporting equipment improvement recommendations (EIR)	R	R	R	R	B.5.2.5	<eir>
Hand receipt (HR) manuals					B.5.2.6	<handreceipt>
Corrosion prevention and control (CPC)	R	R	R	R	B.5.2.7	<cpcdata>
Ozone depleting substances (ODS)					B.5.2.8	<odsdata>
Destruction of Army materiel to prevent enemy use	R	R	R	R	B.5.2.9	<destructmat>
Preparation for storage or shipment	R	R	R	R	B.5.2.10	<pssref>
Warranty information					B.5.2.11	<wrntyref>
Nomenclature cross-reference list					B.5.2.12	<nomenreflist>
List of abbreviations/acronyms	R	R	R	R	B.5.2.13	<loa>
Quality of material	P				B.5.2.15	<qual.mat.info>
Safety, care, and handling					B.5.2.16	<sftyinfo>
Nuclear hardness					B.5.2.17	<hcp>
Calibration					B.5.2.18	<calref>

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
Supporting information for repair parts, special tools, TMDE, and support equipment	P				B.5.2.25	<supdata>
Copyright credit line					B.5.2.26	<copyrt>
EQUIPMENT DESCRIPTION AND DATA WORK PACKAGE	R	R	R	R	B.5.3	<descwp>
Equipment characteristics, capabilities, and features	R	R	R	R	B.5.3.3	<eqpinfo>
Location and description of major components	R	R	R	R	B.5.3.4	<locdesc>
Differences between models					B.5.3.5	<eqpdiff>
Equipment data	R	R	R	R	B.5.3.6	<eqpdata>
THEORY OF OPERATION WORK PACKAGE	R	R	R	R	B.5.4	<thrywp>
CHAPTER X. OPERATOR INSTRUCTIONS	R	R	R	R	C.5.1	<opim>
DESCRIPTION AND USE OF OPERATOR CONTROLS AND INDICATORS WORK PACKAGE	R	R	R	R	C.5.2.3	<ctrlindwp>
OPERATION UNDER USUAL CONDITIONS WORK PACKAGE	R	R	R	R	C.5.2.4	<opusualwp>
Security measures for electronic data					C.5.2.4.3	<secref>
Siting requirements					C.5.2.4.4	<site>
Shelter requirements					C.5.2.4.5	<shelter>
Assembly and preparation for use					C.5.2.4.6	<prepforuse>
Initial adjustments, before use and self-test					C.5.2.4.7	<initial>
Operating procedures	R	R	R	R	C.5.2.4.8	<oper>
Decals and instruction plates					C.5.2.4.8.2	<instructplt>
Operating auxiliary equipment					C.5.2.4.9	<operaux>
Preparation for movement					C.5.2.4.10	<prepmove>
OPERATION UNDER UNUSUAL CONDITIONS WORK PACKAGE	R	R	R	R	C.5.2.5	<opunuwp>
Security measures for electronic data					C.5.2.5.3.1	<secref>
Unusual environment / weather	R	R	R	R	C.5.2.5.3.2	<unusualenv>
Fording and swimming					C.5.2.5.3.3	<fording>
Interim nuclear, biological, and chemical (NBC) decontamination procedures					C.5.2.5.3.4	<decon>

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
Jamming and electronic countermeasures (ECM) procedures					C.5.2.5.3.5	<ecm>
Degraded operation procedures					C.5.2.5.3.6	<degraded>
EMERGENCY WORK PACKAGE					C.5.2.6	<emergencywp>
STOWAGE AND DECAL / DATA PLATE GUIDE WORK PACKAGE					C.5.2.7	<stowagewp>
ON-VEHICLE EQUIPMENT LOADING PLAN WORK PACKAGE					C.5.2.8	<eqploadwp>
CHAPTER X. TROUBLESHOOTING MASTER INDEX					D.5.1 D.5.4.4	<tim> <masterindexcategory>
TROUBLESHOOTING INDEX WORK PACKAGE	R	R	R	R	D.5.5.5	<tsindxwp>
CHAPTER X. TROUBLESHOOTING PROCEDURES ***NOTE*** *The notation (*) indicates that, if required, at least one of the these content items shall be included*		R	R	R	D.5.1 D.5.4.2	<tim> <troublecategory>
TROUBLESHOOTING INDEX WORK PACKAGE					D.5.5.5	<tsindxwp>
**OPERATIONAL CHECKOUT WORK PACKAGES*					D.5.5.8.3	<opcheckwp>
**TROUBLESHOOTING PROCEDURES WORK PACKAGES*					D.5.5.8.4	<tswp>
**COMBINED OPERATIONAL CHECKOUT AND TROUBLESHOOTING PROCEDURES WORK PACKAGES*					D.5.5.8.5	<opcheck-tswp>
CHAPTER X. PMCS MAINTENANCE INSTRUCTIONS ***NOTE*** *PMCS is required as a minimum in one maintenance chapter*					E.5.2 E.5.2.1	<mim> <pmcscategory>
PMCS INTRODUCTION WORK PACKAGE	R	R	R	R	E.5.3.4.1	<pmcsintrowp>
PMCS, INCLUDING LUBRICATION INSTRUCTIONS, WORK PACKAGE	R	R	R	R	E.5.3.4.2	<pmcswp>

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
CHAPTER X. MAINTENANCE INSTRUCTIONS ***NOTE*** *PMCS is required as a minimum in one maintenance chapter*	R	R	R	R	E.5.2 E.5.2.2 E.5.2.3	<mim> <maintenancepmcscategory> <maintenancecategory>
SERVICE UPON RECEIPT WORK PACKAGE	P	R	R	R	E.5.3.2	<surwp>
Siting	P				E.5.3.2.3.1	<siting>
Shelter requirements	P				E.5.3.2.3.2	<shltr>
Service upon receipt of materiel	P	R	R	R	E.5.3.2.3.3	<surmat>
Installation instructions	P	R	R	R	E.5.3.2.3.4	<install>
Preliminary servicing of equipment	P				E.5.3.2.3.5	<preserv>
Preliminary checks and adjustment of equipment	P				E.5.3.2.3.6	<prechkadj>
Preliminary calibration of equipment	P				E.5.3.2.3.7	<precal>
Circuit alignment	P				E.5.3.2.3.8	<calign>
Ammunition markings	P				E.5.3.2.3.9.1	<ammo.markings>
Classification of defects	P				E.5.3.2.3.9.2	<ammo.defect>
Ammunition handling	P				E.5.3.2.3.9.3	<ammo.handling>
Procedures to activate ammunition	P				E.5.3.2.3.9.4	<arm>
Other service upon receipt task	P				E.5.3.2.3.10	<other.surtsk>
Follow-on maintenance	P				E.5.3.2.3.11	<followon.maintsk>
EQUIPMENT / USER FITTING INSTRUCTIONS WORK PACKAGE (PERSONAL USE EQUIPMENT)	P				E.5.3.3	<perseqpwp>
PMCS INTRODUCTION WORK PACKAGE	R	R	R	R	E.5.3.4.1	<pmcsintrowp>
PMCS, INCLUDING LUBRICATION INSTRUCTIONS, WORK PACKAGE	R	R	R	R	E.5.3.4.2	<pmcswp>
MAINTENANCE WORK PACKAGES ***NOTE*** *As applicable, the following maintenance tasks shall be presented in the general order listed below:*	R	R	R	R	E.5.3.5	<maintwp>
Servicing					E.5.3.5.3.3	<service>
Ground handling					E.5.3.5.3.4	<groundtsk>
Inspection of installed items					E.5.3.5.3.5	<inspinstitm>

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
Removal					E.5.3.5.3.6	<remove>
Disassembly					E.5.3.5.3.7	<disassem>
Cleaning					E.5.3.5.3.8	<clean>
Inspection-acceptance and rejection criteria					E.5.3.5.3.9	<acptrejinsp>
Nondestructive testing inspection (NDTI)					E.5.3.5.3.10	<ndti>
Repair or replacement					E.5.3.5.3.11	<repair-rplc>
Alignment					E.5.3.5.3.12	<align>
Painting					E.5.3.5.3.13	<paint>
Lubrication					E.5.3.5.3.14	<lube>
Assembly					E.5.3.5.3.15	<assem>
Test and inspection					E.5.3.5.3.16	<test-inspect>
Installation					E.5.3.5.3.17	<install>
Adjustment					E.5.3.5.3.18	<adjust>
Calibration					E.5.3.5.3.19	<calibration>
Radio interference suppression					E.5.3.5.3.20	<ris>
Placing in service					E.5.3.5.3.21	<pis>
Testing					E.5.3.5.3.22	<test-pass>
Preparation for storage or shipment					E.5.3.5.3.25	<pss>
Classification of defects					E.5.3.5.3.26	<ammo.defect>
Handling ammunition					E.5.3.5.3.27	<ammo.handling>
Ammunition markings					E.5.3.5.3.28	<ammo.markings>
Procedures for ammunition activation					E.5.3.5.3.29	<arm>
Additional maintenance task					E.5.3.5.3.30	<other.maintsk>
Follow-on maintenance					E.5.3.5.3.31	<followon.maintsk>
GENERAL MAINTENANCE WORK PACKAGE					E.5.3.6	<maintwp>
LUBRICATION INSTRUCTIONS WORK PACKAGE					E.5.3.7	<lubewp>
ILLUSTRATED LIST OF MANUFACTURED ITEMS WORK PACKAGE	P				E.5.3.9	<manuwp>
TORQUE LIMITS WORK PACKAGE	P				E.5.3.10	<torquewp>
WIRING DIAGRAMS WORK PACKAGE	P				E.5.3.11	<wiringwp>

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
CHAPTER X. **AUXILIARY EQUIPMENT** **MAINTENANCE INSTRUCTIONS**					E.5.2 E.5.2.6	<mim> <auxiliarycategory>
AUXILIARY EQUIPMENT MAINTENANCE WORK PACKAGE					E.5.3.13	<auxeqpwp>
ILLUSTRATED LIST OF MANUFACTURED ITEMS WORK PACKAGE	P				E.5.3.9	<manuwp>
TORQUE LIMITS WORK PACKAGE	P				E.5.3.10	<torquewp>
WIRING DIAGRAMS WORK PACKAGE	P				E.5.3.11	<wiringwp>
CHAPTER X. **AMMUNITION** **MAINTENANCE INSTRUCTIONS**					E.5.2 E.5.2.7	<mim> <ammunitioncategory>
AMMUNITION MAINTENANCE WORK PACKAGE					E.5.3.14.1	<ammowp>
AMMUNITION MARKING INFORMATION WORK PACKAGE	P				E.5.3.14.2	<ammo.markingwp>
FOREIGN AMMUNITION (NATO) WORK PACKAGE	P				E.5.3.14.3	<natowp>
CHAPTER X. **PARTS INFORMATION** *(-10 THROUGH -14)* *(-12&P THROUGH -14&P)*	 P P	 P R	 P R	 P R	F.5.3.2	<pim>
INTRODUCTION WORK PACKAGE	P	R	R	R	F.5.3.5	<introwp>
REPAIR PARTS LIST WORK PACKAGE	P	R	R	R	F.5.3.6	<plwp>
REPAIR PARTS FOR SPECIAL TOOLS WORK PACKAGE	P				F.5.3.7	<stl_partswp>
KIT PARTS LIST WORK PACKAGE	P				F.5.3.8	<kitswp>
BULK ITEM WORK PACKAGE	P				F.5.3.9	<bulk_itemswp>
SPECIAL TOOLS LIST WORK PACKAGE	P				F.5.3.10	<stlwp>
NSN INDEX WORK PACKAGE	P	R	R	R	F.5.3.11.1	<nsnindxwp>
P/N INDEX WORK PACKAGE	P	R	R	R	F.5.3.11.2	<pnindxwp>
REFERENCE DESIGNATOR INDEX WORK PACKAGE	P				F.5.3.11.3	<refdesindxwp>

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
CHAPTER X. SUPPORTING INFORMATION ***NOTE*** *Applicable supporting information work packages shall be arranged in the order in which they are presented here and numbered accordingly.*	R	R	R	R	G.5.1	<sim>
REFERENCES WORK PACKAGE	R	R	R	R	G.5.2	<refwp>
INTRODUCTION FOR STANDARD MAC WORK PACKAGE *(FIVE-LEVEL MAINTENANCE ONLY)* *OR* *(TWO-LEVEL MAINTENANCE ONLY)*	P	R	R	R	G.5.3.1 G.5.3.3	<macintrowp>
MAC WORK PACKAGE (FIVE-LEVEL MAINTENANCE ONLY) *OR* *(TWO-LEVEL MAINTENANCE ONLY)*	P	R	R	R	G.5.3.4	<macwp>
COMPONENTS OF END ITEM (COEI) AND BASIC ISSUE ITEMS (BII) LISTS WORK PACKAGE	R	R	R	R	G.5.4	<coeibiiwp>
ADDITIONAL AUTHORIZATION LIST (AAL) WORK PACKAGE					G.5.5	<aalwp>
EXPENDABLE AND DURABLE ITEMS LIST WORK PACKAGE	R	R	R	R	G.5.6	<explistwp>
TOOL IDENTIFICATION LIST WORK PACKAGE	P				G.5.7	<toolidwp>
MANDATORY REPLACEMENT PARTS WORK PACKAGE	P				G.5.8	<mrplwp>
CRITICAL SAFETY ITEMS AND FLIGHT SAFETY CRITICAL AIRCRAFT PARTS WORK PACKAGE					G.5.9	<csi.fscap.wp>
SUPPORT ITEMS WORK PACKAGE					G.5.10	<supitemwp>
ADDITIONAL SUPPORTING WORK PACKAGES					G.5.11	<genwp>
REAR MATTER	R	R	R	R	5.2.2	<rear>
Glossary		R			5.2.2.1	<glossary>
Alphabetical index		R			5.2.2.2	<aindx>
DA Form 2028	R	R	R	R	5.2.2.3	<da2028>

TM Requirements Matrix for TM 5-6350-XXX-12&P .

TM Content	-10	-12 -12&P	-13 -13&P	-14 -14&P	MIL-STD-40051-2 Reference	Element Name
Authentication page	R	R	R	R	5.2.2.4	<authent>
Foldout pages					5.2.2.5	<foldsect>
Back cover	R	R	R	R	5.2.2.6	<back>

Legend

R Required

P Prohibited

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 1 SENSOR: BMS with self test

MODEL: SENTROL 2706AP OR EQUAL

DESCRIPTION. THE BALANCED MAGNETIC SWITCH (BMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT THE OPENING OF A DOOR OR WINDOW. IN A TYPICAL APPLICATION, THE SWITCH ASSEMBLY IS MOUNTED TO THE DOOR FRAME AND THE ACTUATING MAGNET ASSEMBLY IS MOUNTED TO THE DOOR. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR THE STANDARD CONFIGURATION SENSOR WITH SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 634)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - CHANGE IN THE MAGNETIC FIELD CAUSED BY .80 $\pm$ 0.40 INCH IN SEPARATION OF THE MAGNETS - LOCAL MAGNETIC FIELD HAS A POSITIVE OR NEGATIVE DIFFERENCE FROM THE FIELD AT THE TIME OF ADJUSTMENT; GREATER THAN 67 GAUSS
5. TAMPER PROTECTION - MEET UL 634
6. SENSOR STIMULUS - ALLOWS THE SENSOR TO BE TESTED FROM A REMOTE LOCATION
7. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME
OR
EQUAL ITEMS

PES: 2 SENSOR: BMS without self test

MODEL: SENTROL 2707A OR EQUAL

DESCRIPTION. THE BALANCED MAGNETIC SWITCH (BMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT THE OPENING OF A DOOR OR WINDOW. IN A TYPICAL APPLICATION, THE SWITCH ASSEMBLY IS MOUNTED TO THE DOOR FRAME AND THE ACTUATING MAGNET ASSEMBLY IS MOUNTED TO THE DOOR. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR THE STANDARD CONFIGURATION SENSOR WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 634)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - CHANGE IN THE MAGNETIC FIELD CAUSED BY .80 $\pm$ 0.40 INCH IN SEPARATION OF THE MAGNETS - LOCAL MAGNETIC FIELD HAS A POSITIVE OR NEGATIVE DIFFERENCE FROM THE FIELD AT THE TIME OF ADJUSTMENT; GREATER THAN 67 GAUSS
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME
OR
EQUAL ITEMS

PES: 3 SENSOR: BMS LOW PROFILE without self test

MODEL: SENTROL 2727A OR EQUAL

DESCRIPTION. THE BALANCED MAGNETIC SWITCH (BMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT THE OPENING OF A DOOR OR WINDOW. IN A TYPICAL APPLICATION, THE SWITCH ASSEMBLY IS MOUNTED TO THE DOOR FRAME AND THE ACTUATING MAGNET ASSEMBLY IS MOUNTED TO THE DOOR. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR THE LOW-PROFILE HERMETICALLY SEALED CONFIGURATION SENSOR WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 634)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - CHANGE IN THE MAGNETIC FIELD CAUSED BY .80 $\pm$ 0.40 INCH IN SEPARATION OF THE MAGNETS - LOCAL MAGNETIC FIELD HAS A POSITIVE OR NEGATIVE DIFFERENCE FROM THE FIELD AT THE TIME OF ADJUSTMENT; GREATER THAN 67 GAUSS
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
7. LOW PROFILE CONSTRUCTION - DESIGNED FOR OVERHEAD DOORS

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME
OR
EQUAL ITEMS

PES: 4 SENSOR: PIMS(V) with self test

MODEL: SENTROL 6187CTX-N6 OR EQUAL

DESCRIPTION. THE VOLUMETRIC OR WIDE ANGLE PASSIVE INFRARED MOTION SENSOR (PIMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT A MOVING INTRUDER WITHIN THE FIELD OF VIEW. IN A TYPICAL APPLICATION, THE PIMS IS MOUNTED ON A STURDY WALL ABOVE HEAD HEIGHT. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR A VOLUMETRIC SENSOR WITH SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - VELOCITY 0.4 FT/SEC TO 8 FT/SEC - AT ALL RANGES FROM 6 FT UP TO 30 FT - ON ALL AZIMUTH ANGLES BETWEEN +/- 45 DEGREES FROM BORE SIGHT
5. TAMPER PROTECTION - MEET UL 634
6. SENSOR STIMULUS - ALLOWS SENSOR TO BE TESTED FROM A REMOTE LOCATION
7. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
8. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc
9. SENSITIVITY ADJUSTMENT - AT LEAST TWO LEVELS

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 5 SENSOR: PIMS(V) without self test

MODEL: SENTROL 6187CTX OR EQUAL

DESCRIPTION. THE VOLUMETRIC OR WIDE ANGLE PASSIVE INFRARED MOTION SENSOR (PIMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT A MOVING INTRUDER WITHIN THE FIELD OF VIEW. IN A TYPICAL APPLICATION, THE PIMS IS MOUNTED ON A STURDY WALL ABOVE HEAD HEIGHT. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR A VOLUMETRIC SENSOR WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - VELOCITY O.4 FT/SEC TO 8 FT/SEC - AT ALL RANGES FROM 6 FT UP TO 30 FT - ON ALL AZIMUTH ANGLES BETWEEN +/- 45 DEGREE FROM BORE SIGHT
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
7. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc
8. SENSITIVITY ADJUSTMENT - AT LEAST TWO LEVELS

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 6 SENSOR: PIMS(C) with self test

MODEL: SENTROL 6187CTX-N6 OR EQUAL

DESCRIPTION. THE CURTAIN PASSIVE INFRARED MOTION SENSOR (PIMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT A MOVING INTRUDER WITHIN THE FIELD OF VIEW. IN A TYPICAL APPLICATION, THE CURTAIN PIMS IS MOUNTED ON A STURDY WALL ABOVE HEAD HEIGHT. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR A CURTAIN SENSOR WITH SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - VELOCITY O.4 FT/SEC TO 11 FT/SEC - AT ALL RANGES FROM 6 FT UP TO 30 FT - ON ALL AZIMUTH ANGLES BETWEEN +/- 3 DEGREES FROM BORE SIGHT.
5. TAMPER PROTECTION - MEET UL 634
6. SENSOR STIMULUS - ALLOWS SENSOR TO BE TESTED FROM A REMOTE LOCATION
7. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
8. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 7 SENSOR: PIMS(C) without self test

MODEL: SENTROL 6187CTX/6073 OR EQUAL

DESCRIPTION. THE CURTAIN PASSIVE INFRARED MOTION SENSOR (PIMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT A MOVING INTRUDER WITHIN THE FIELD OF VIEW. IN A TYPICAL APPLICATION, THE PIMS IS MOUNTED ON A STURDY WALL ABOVE HEAD HEIGHT. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR A CURTAIN SENSOR WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - VELOCITY 0.4 FT/SEC TO 11 FT/SEC - AT ALL RANGES FROM 6 FT UP TO 30 FT - ON ALL AZIMUTH ANGLES BETWEEN +/- 3 DEGREES FROM BORE SIGHT
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
7. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 8 SENSOR: PIMS(O) with self test

MODEL: PULNIX 7100-ET OR EQUAL

DESCRIPTION. THE OMNI-DIRECTIONAL PASSIVE INFRARED MOTION SENSOR (PIMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT A MOVING INTRUDER WITHIN THE FIELD OF VIEW. IN A TYPICAL APPLICATION, THE PIMS IS MOUNTED ON THE CEILING. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR AN OMNI-DIRECTIONAL SENSOR WITH SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - VELOCITY 0.4 FT/SEC TO 9 FT/SEC - AT ALL RANGES UP TO 20 FT @ HGT 9'1" - AT ALL ANGLES ABOUT A LINE THROUGH A POINT DIRECTLY BELOW THE SENSOR
5. TAMPER PROTECTION - MEET UL 634
6. SENSOR STIMULUS - ALLOWS SENSOR TO BE TESTED FROM A REMOTE LOCATION
7. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
8. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc
9. SENSITIVITY ADJUSTMENT - AT LEAST TWO LEVELS

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 9 SENSOR: PIMS(O) without self test

MODEL: PULNIX PA7100-ET OR EQUAL

DESCRIPTION. THE OMNI-DIRECTIONAL PASSIVE INFRARED MOTION SENSOR (PIMS) IS AN INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT A MOVING INTRUDER WITHIN THE FIELD OF VIEW. IN A TYPICAL APPLICATION, THE PIMS IS MOUNTED ON THE CEILING. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR AN OMNI-DIRECTIONAL SENSOR WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - VELOCITY 0.4 FT/SEC TO 9 FT/SEC - AT ALL RANGES UP TO 20 FT @ HGT 9'1" - AT ALL ANGLES ABOUT A LINE THROUGH A POINT DIRECTLY BELOW THE SENSOR
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
7. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc
8. SENSITIVITY ADJUSTMENT - AT LEAST TWO LEVELS

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME
OR
EQUAL ITEMS

PES: 10 SENSOR: Dual Technology (HS) – Microwave and Infrared

MODEL: PROTECH SDI-76M-HS1 OR EQUAL

DESCRIPTION. THE DUAL TECHNOLOGY SENSOR (HS) UTILIZES A MICROWAVE MOTION SENSOR (MMS) AND A PASSIVE INFRARED MOTION SENSOR (PIMS) TO SATISFY THE HIGH SECURITY REQUIREMENT. IT IS INTENDED TO DETECT A MOVING PERSON. IN A TYPICAL APPLICATION, THE HS IS MOUNTED ON A WALL ABOVE HEAD HEIGHT AND PROTECTS A VOLUME DIRECTLY IN FRONT AND TO BOTH SIDES. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR HS SENSOR OPERATING WITH OR WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORETHAN 1 IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - VELOCITY O.3 FT/SEC TO 15 FT/SEC AT ALL RANGES UP TO 30 FT.
5. HIGH SECURITY FEATURES - AND /OR GATED SWITCHABLE ANTI MASKING – REMOTE POWER SHUTOFF
6. TAMPER PROTECTION - MEET UL 634
7. OPERATIONAL POWER – 10.5 - 20 VOLTS DC
8. POWER CONSUMPTION - 130mA @ 12 Vdc
9. SENSITIVITY ADJUSTMENT - PROVIDES FIELD ADJUSTABLE SENSITIVITY AND RANGE CONTROLS.

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 11 SENSOR: VS with self test

MODEL: SENTROL DV1200 SERIES ADVISOR X OR EQUAL

DESCRIPTION. THE VIBRATION SENSOR (VS) IS DESIGNED TO DETECT FORCED PENETRATION IN VAULTS, SAFES, OR OTHER REINFORCED AREAS. IN A TYPICAL APPLICATION, THE VS IS MOUNTED ON THE SURFACES, WALLS, OR CEILINGS TO BE PROTECTED. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR VS SENSOR WITH SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - SHALL DETECT VIBRATION CAUSED BY HAMMERING, DRILLING, CUTTING TOOLS, ETC DETECTION RANGE: REINFORCED CONCRETE - 10 FT RADIUS; CINDER BLOCK MTD ON REINFORCED PORTION - 5 FT RADIUS; CINDER BLOCK MTD ON HOLLOW PORTION - 40 INCHES RADIUS
5. TAMPER PROTECTION - MEET UL 634
6. SENSOR STIMULUS - ALLOWS SENSOR TO BE TESTED FROM A REMOTE LOCATION
7. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
8. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc
9. SENSITIVITY ADJUSTMENT - 5 STEPS OF 6 dB - 30 dB

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 12 SENSOR: DS

MODEL: ADEMCO 269 OR EQUAL

DESCRIPTION. THE DURESS ALARM SWITCH (DS) IS INTENDED TO PROVIDE THE MEANS TO COVERTLY NOTIFY THE ALARM ANNUNCIATION SYSTEM THAT A DURESS SITUATION EXISTS. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR A DS SENSOR WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - ALL ACTIVATION
3. FALSE ALARM PERFORMANCE - NONE
4. ALARM CRITERIA: - TO BE ACTUATED DIRECTLY ; NO VISIBLE OR AUDIBLE ALARM FROM THE SWITCH; SWITCH SHALL LOCK UNTIL MANUALLY RESET
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
7. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 13 SENSOR: GBS without self test

MODEL: SENTROL SHATTERPRO-5810 OR EQUAL

DESCRIPTION. THE GLASS BREAK SENSOR (GBS) IS DESIGNED TO DETECT THE AIRBORNE OR ACOUSTIC ENERGY RESULTING FROM THE BREAKING OF SINGLE AND DOUBLE STRENGTH PLATE, FLOAT, LAMINATED, TEMPERED, AND WIRED GLASS. THE GBS IS A STAND-OFF DETECTOR AND, IN A TYPICAL APPLICATION, THE GBS IS MOUNTED ON THE WALLS OR CEILINGS OF THE SECURE AREA TO BE PROTECTED. THE FOLLOWING SALIENT CHARACTERISTICS ARE FOR A GBS WITHOUT SELF-TEST CAPABILITY:

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN ONE IN A PERIOD OF 480 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA: - SHALL DETECT ACOUSTIC ENERGY RESULTING FROM THE BREAKING OF SINGLE AND DOUBLE STRENGTH PLATE, FLOAT, LAMINATED, TEMPERED, AND WIRED GLASS; WITHIN 20 FOOT RADIUS OF COVERAGE FROM THE BREAKING GLASS.
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER - 12 VOLTS DC (-4,+8)
7. POWER CONSUMPTION - LESS THAN 25mA @ 12 Vdc

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 21 SENSOR: EMMS

MODEL: RACON 14100 OR EQUAL

DESCRIPTION. THE EXTERIOR MICROWAVE MOTION SENSOR (EMMS) IS A BISTATIC EXTERIOR PERIMETER INTRUSION DETECTION SENSOR. IT IS INTENDED TO DETECT A PERSON OR VEHICLE MOVING THROUGH ITS ZONE OF DETECTION. IN A TYPICAL APPLICATION, THE PRODUCT IS MOUNTED NEAR OR BETWEEN FENCE LINES TO PROTECT THE PERIMETER OF AN AREA.

SALIENT CHARACTERISTICS:

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA - VELOCITY 0.1 FT/SEC TO 15 FT/SEC (88 FT/SEC FOR VEHICLES) AT ALL RANGES UP TO 330 FT
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC OUTPUT 13.6 VDC
7. POWER CONSUMPTION – 11 VDC TO 15 VDC @ 100 MA
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 22 SENSOR: IPS

MODEL: PULNIX PB-100AT (ANTI CRAWL) OR EQUAL

DESCRIPTION. THE EXTERIOR INFRARED PERIMETER SENSOR (IPS) IS A PEDESTAL MOUNTED, ACTIVE INTRUSION SENSOR CONSISTING OF A TRANSMITTER AND RECEIVER MOUNTED IN TWO EXTERIOR POST TYPE HOUSINGS. THE TRANSMITTER CONSISTS OF MULTIPLE MODULATED OR PULSED INFRARED BEAM EMITTING TRANSMITTERS. THE RECEIVER CONSISTS OF MULTIPLE INFRARED BEAM COLLECTING RECEIVERS. AN ALARM IS GENERATED WHEN A PERSON OR VEHICLE MOVES THROUGH THE ZONE OF DETECTION INTERRUPTING THE BEAM BETWEEN A TRANSMITTER AND A RECEIVER OR DISTURBING THE BEAM MODULATION. CONFIGURATION IS OPTIMIZED TO DETECT CRAWLING INTRUDERS.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA - VELOCITY O.1 FT/SEC TO 88 FT/SEC AT ALL RANGES UP TO 330 FT
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION – 12-30 VDC <105 MA PER UNIT
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS IIi BRAND NAME OR EQUAL ITEMS

PES: 23 SENSOR: FMVS

MODEL: RACON Fence Guard F-100 OR EQUAL

DESCRIPTION. THE FENCE MOUNTED VIBRATION SENSOR (FMVS) IS AN EXTERIOR INTRUSION DETECTION SENSOR. IT IS NORMALLY MOUNTED ON A CHAINLINK FENCE TO DETECT MOTION SUCH AS INTRUDER CLIMBING, PULLING, AND CUTTING. WHEN THE VIBRATION SIGNALS EXCEED A PRESET THRESHOLD AND OTHER PRESET CONDITIONS AN ALARM WILL RESULT.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERIONOCCURS
4. ALARM CRITERIA – INTRUSION ATTEMPTS BY PULLING, TUGGING, CUTTING, OR CLIMBING THE FENCE WILL BE DETECTED FOR TWO 100 METER MINIMUM ZONES
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION – 12 VDC @<115 MA
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 24 SENSOR: SSCF

MODEL: PERIMETER PRODUCTS FPS-2 OR EQUAL

DESCRIPTION. THE STRAIN SENSITIVE CABLE FENCE (SSCF) SENSOR IS AN EXTERIOR INTRUSION DETECTION SENSOR THAT ATTACHES TO A FENCE (CHAINLINK). IT IS DESIGNED TO DETECT INTRUDER ATTEMPTS TO CLIMB, CUT, OR LIFT THE FENCE FABRIC. EACH SENSOR PROCESSOR CAN PROTECT TWO 330 FT ZONES.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA – INTRUSION ATTEMPTS BY PULLING, TUGGING, CUTTING, OR CLIMBING THE FENCE WILL BE DETECTED FOR TWO 330 FT ZONES
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION – 12 VDC @ 100 MA
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 25 SENSOR: TWFS

MODEL: MAGAL DTR-2000 OR EQUAL

DESCRIPTION. THE TAUT WIRE FENCE SENSOR (TWFS) IS AN EXTERIOR SENSOR USING TENSIONED BARBED WIRE DISPLACEMENT TO DETECT INTRUSION ATTEMPTS BY CUTTING, PULLING, OR A FENCE CLIMBING INTRUDER. THE SENSOR CAN BE ATTACHED TO VERICAL OR Y OUTRIGGERS.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA – A LATERAL FORCE OF 30 POUNDS APPLIED TO ANY STRAND OF THE BARBED WIRE OR A 6 INCH LATERAL DEFLECTION OF ANY STRAND WILL GENERATE AN ALARM
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 115/230 VAC 50-6- HZ
7. POWER CONSUMPTION – 6 WATTS MAX.
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 26 SENSOR: PCCS

MODEL: SENSTAR STELLAR “PERIMITRAX” OR EQUAL

DESCRIPTION. THE PORTED COAX CABLE SENSOR (PCCS) IS AN EXTERIOR BURIED LINE SENSOR DESIGNED TO DETECT HUMANS AND VEHICLES CROSSING THE DETECTION ZONE. THE SENSOR USES A PAIR* OF COAXIAL CABLES BURIED PARALLEL TO EACH OTHER ALONG THE PERIMETER. WHEN AN INTRUDER DISTURBS THE ELECTROMAGNETIC FIELD BETWEEN THE CABLES, AN ALARM IS GENERATED. EACH SENSOR PROCESSOR CAN CONTROL 2 ZONES. EACH ZONE MAY BE UP TO 200 METERS IN LENGTH.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA – MOTION OF A HUMAN INTRUDER BETWEEN 0.05 AND 8 METERS/SECOND SHALL GENERATE AN ALARM.
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION – WITH BATTERY BACKUP. 12 VDC @500 MA
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 27 SENSOR: RF FIELD DISTURBANCE SENSOR

MODEL: AURATEK “ENCLOSURE” FSP-300 OR EQUAL

DESCRIPTION. THE RF FIELD DISTURANCE SENSOR IS AN EXTERIOR SENSOR INTENDED FOR PERIMETER PROTECTION BY DETECTING AN INTRUDER APPROACHING OR CROSSING THE DETECTION ZONE. THE SENSOR USES A STANDARD COAXIAL CABLE THAT MAY BE SURFACE DEPLOYED, BURIED, OR ATTACHED TO A BARRIER ALONG THE PERIMETER. THE SENSOR FIELD IS ESTABLISHED USING A SELF CONTAINED. MULTI-FREQUENCY FM TRANSMITTER. THE RF FIELD IS ESTABLISHED USING EITHER TWO CABLES PER ZONE OR ONE CABLE PER ZONE AND AN ANTENNA. EACH SENSOR PROCESSOR CAN PROTECT 2 ZONES OF UP TO 150 METERS EACH.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA – MOTION OF A HUMAN INTRUDER BETWEEN 0.05 AND 8 METER/SECOND (0.15 – 26 FT/SEC) SHALL GENERATE AN ALARM.
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION – 11 - 18 VDC @2.0 A. BATTERY BACKUP IS AVAILABLE
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 28 SENSOR: FOPS

MODEL: FIBER SENSYS, INC. DEFENDER MODEL 205 OR EQUAL

DESCRIPTION. THE FIBEROPTIC PERIMETER SENSOR (FOPS) IS AN EXTERIOR INTRUSION DETECTION SENSOR THAT MAY BE MOUNTED ON FENCES,WALLS, ROOFTOPS, OR BURIED UNDER GRAVEL OR SOD. UTILIZING ADVANCED SIGNAL PROCESSING, THE SENSOR IS DESIGNED TO DETECT HUMANS CROSSING THE DETECTION ZONE. THE SENSOR USES FIBER OPTIC CABLE THAT DETECTS MOTION, VIBRATION, AND CHANGES IN PRESSURE. WHEN AN INTRUDER CROSSES THE DETECTION ZONE. EACH SENSOR CAN PROTECT A ZONE UP TO A MAXIMUM LENGTH OF 1981 METERS.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA – MOTION OF A HUMAN INTRUDER BETWEEN 0.1 AND 8 METERS/SECOND SHALL GENERATE AN ALARM.
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION 10 – 26 VDC. 1.5 WATT TYPICAL
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 29 SENSOR: FMVSS

MODEL: SOUTHWEST MICROWAVE INTREPID™ OR EQUAL

DESCRIPTION. THE FENCE MOUNTED VIBRATION SENSOR SYSTEM, (FMVSS), IS AN EXTERIOR INTRUSION DETECTION SENSOR SYSTEM. IT IS MOUNTED ON A CHAINLINK FENCE TO DETECT MOTION SUCH AS INTRUDER CLIMBING, PULLING, AND CUTTING. WHEN THE VIBRATION SIGNALS EXCEED A PRESET THRESHOLD AND OTHER PRESET CONDITIONS, AN ALARM WILL RESULT. THE FMVSS IS INSENSITIVE TO NOISE DUE TO WIND AND RAIN. IT AUTOMATICALLY COMPENSATES FOR VARIATIONS IN THE FENCE CONDITION.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA – INTRUSION ATTEMPTS BY PULLING, TUGGING, CUTTING, OR CLIMBING THE FENCE WILL BE DETECTED. EACH PROCESSOR HANDLES DATA FROM TWO LENGTHS OF CABLE. EACH CABLE MAY BE UP TO 200 METERS LONG. UP TO EIGHT PROCESSORS MAY BE LINKED FOR LONG PERIMETERS.
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION PROCESSOR – 12 VDC @ 470 MA
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL

PERFORMANCE EQUIVALENCE SHEET (PES) FOR ICIDS III BRAND NAME OR EQUAL ITEMS

PES: 30 SENSOR: FMVSS

MODEL: FIBER SENSYS, INC COPPERHEAD™ CH402KT OR EQUAL

DESCRIPTION. THE FENCE MOUNTED VIBRATION SENSOR SYSTEM, (FMVSS), IS AN EXTERIOR INTRUSION DETECTION SENSOR SYSTEM. IT UTILIZES PIEZOELECTRIC CABLE MOUNTED ON A CHAINLINK FENCE TOGETHER WITH ADVANCED DIGITAL SIGNAL PROCESSING (DSP) TO DETECT MOTION SUCH AS INTRUDER CLIMBING, PULLING, AND CUTTING. THE DSP UTILLIZES SPECIAL ALGORITHMS TO REJECT TO NOISE DUE TO WIND AND RAIN. WIND REJECTION CAPABILITY CONTINUOUSLY OPTIMIZES SENSOR PERFORMANCE WITHOUT EXTERNAL ANEMOMETERS OR WEATHER STATIONS.

SALIENT CHARACTERISTICS

1. UL LISTED (UL 639)
2. DETECTION PERFORMANCE - 99 OF 100 INTRUSION ATTEMPTS SHALL BE DETECTED
3. FALSE ALARM PERFORMANCE - SHALL NOT GENERATE MORE THAN 1 IN A PERIOD OF 2 DAYS IF NO ALARM CRITERION OCCURS
4. ALARM CRITERIA – INTRUSION ATTEMPTS BY PULLING, TUGGING, CUTTING, OR CLIMBING THE FENCE WILL BE DETECTED AND LOCATED WITHIN TWO ZONES FOR EACH PROCESSOR. EACH ZONE IS 100 METERS LONG (MAX 500 M). INSENSITIVE REGIONS MAY BE PROVIDED ANYWHERE IN THE ZONE. UP TO 500 METERS.
5. TAMPER PROTECTION - MEET UL 634
6. OPERATIONAL POWER – INPUT 110/220 VAC
7. POWER CONSUMPTION 10 – 26 VDC @ 1.5 WATTS TYPICAL
8. SENSITIVITY ADJUSTMENT - PROVIDE A FIELD ADJUSTABLE SENSITIVITY CONTROL